

Deniable, Disposable, Disruptive: Iran's Hybrid Warfare in Europe Demands a Proactive Response

by [Adrian Shtuni \(/experts/adrian-shtuni\)](#)

May 4, 2026

ABOUT THE AUTHORS

[Adrian Shtuni \(/experts/adrian-shtuni\)](#)

Adrian Shtuni is the CEO of Shtuni Consulting LLC and an associate fellow with the International Centre for Counter-Terrorism.



Brief Analysis

The low-sophistication, high-volume approach used in wartime attacks claimed by the front group HAYI has exposed critical vulnerabilities in Western efforts to harden soft targets, curb online recruitment, and protect Jewish communities amid spillover from the Middle East.

At the outset of the Iran war, many expected the regime to activate long-embedded sleeper cells abroad. Instead, a leaner, more disposable hybrid operational model has emerged, centered on the front entity Harakat Ashab al-Yamin al-Islamiyah (HAYI). This model relies on the recruitment of non-ideological local residents—mainly youths with petty criminal backgrounds—via casual, gig-economy channels on Snapchat and Telegram. Recruits are offered modest cash incentives for low-complexity acts of violence and intimidation against Jewish communities and symbolic targets in Europe, using readily available materials. Although no fatalities have resulted from these claimed incidents so far, they have achieved measurable psychological and media effects.

HAYI can be considered an Iranian regime proxy in part because its methods mirror Tehran's longstanding practice of outsourcing violence to criminals, gangs, and other local elements for deniability. The group has claimed seventeen incidents across seven European countries since the war began, displaying geographic reach, operational coordination, and calibrated low-damage tactics typical of the hybrid warfare model practiced and exported by Iran's Islamic Revolutionary Guard Corps (IRGC). This performance far exceeds what any genuine new "grassroots group" could achieve in such a short period. Rapid amplification of HAYI's claims through pro-Iranian and "axis of resistance" networks—notably without Sunni jihadist involvement—further indicates its role as an Iranian proxy.

Although some HAYI operatives have been arrested, the group has revealed persistent vulnerabilities in Europe by continuing to access soft targets and exploit online recruitment pipelines that supply a steady stream of disposable local agents. The following analysis draws on a detailed review of HAYI's claimed incidents and provides recommendations for addressing this evolving hybrid threat.

Emergence, Operational Trends, and Responses

HAYI emerged in early March shortly after the war began. Its first claimed attack was an explosion at a synagogue in Liege, Belgium, on March 9. Further incidents were claimed in mid-March, followed by a brief lull and then renewed clusters in mid-April, suggesting a calibrated effort to maintain pressure without overextending resources. Most recently, the group claimed the April 29 London stabbing attack in which two Jewish men were injured (see below for more on this incident).

HAYI has concentrated on Jewish population centers across Western Europe, with London as the primary hub (seven incidents) and the Dutch cities of Rotterdam, Amsterdam, and Nijkerk as initial testing grounds. Early attack claims were also linked to Belgium (Liege, Antwerp), France (Paris), Germany (Munich), Greece (location unspecified), and North Macedonia (Skopje). This progression toward the United Kingdom reflects deliberate targeting of highly symbolic urban centers with sizable Jewish communities. Specific target selection has been symbolic and psychological as well, including five synagogues (Liege, Rotterdam, Skopje, and two in London), various other Jewish or Israeli-linked sites (e.g., schools, community buildings, medical services), and distinctive secondary targets (e.g., U.S. financial institutions, Iranian opposition media). The emphasis remains on intimidation and spectacle rather than mass casualties, thereby facilitating rapid production of video propaganda.

If HAYI's claims of carrying out the London stabbing attack prove true, it would represent a significant operational escalation. The group's established modus operandi has consisted of low-damage incidents targeting property rather than people, evolving from small explosives using basic materials to nighttime arson attacks. HAYI also claimed an apparently fake incident involving a drone carrying purported "radioactive and carcinogenic" materials near the Israeli embassy in London. These claimed operations appear to prioritize accessibility, low cost, and ease of documentation and propaganda exploitation. Moreover, the devices used in some incidents have failed, highlighting significant operational limitations.

In contrast, the London stabbing attack was a high-risk daytime assault against multiple individuals with a substantial likelihood of injury or death. This fits the profile of a lone or opportunistic actor far better than HAYI's pattern of low-effort harassment and arson. The suspect—Essa Suleiman, a 45-year-old Somali-born British national with a history of violence (including a 2008 stabbing of a police officer), mental health issues, and a prior referral under the government's Prevent program—is unlikely to have been an ordinary, low-paid HAYI hire. Indeed, without conclusive evidence that the assailant was directed by HAYI, this claim should be treated with caution.

When conducting information operations or announcing claims of responsibility, HAYI lacks a dedicated media outlet of its own. Instead, its videos are circulated and amplified primarily through Telegram channels that are either directly supportive of the Iranian regime or linked to groups within Tehran's so-called axis of resistance, especially Iraqi Shia militias. This layered setup further facilitates both deniability and dissemination, as these axis groups tend to have their own established branding, local legitimacy, and media channels.

HAYI's short clips typically feature shaky cellphone footage of the alleged incidents overlaid with its emblem: a green-tinted hand gripping a scoped SVD Dragunov rifle against a waving red flag with Shia-style Arabic calligraphy. Modeled on the visual style of axis groups like Lebanese Hezbollah, the Yemeni Houthis, and Iraqi Kataib Hezbollah, this design draws from the shared language of Iran-linked organizations while sharply contrasting with Sunni jihadist organizations, which overwhelmingly use black flags bearing the Shahada in white.

As of April 29, authorities had made at least forty-four arrests in connection with HAYI incidents: twenty-eight in the UK, ten in the Netherlands, four in France, and two in Belgium. The majority of them were young men, including eleven boys age 14 to 17; three women age 47 to 59 have been arrested as well. At least sixteen individuals have been formally charged: eight in the UK, four in the Netherlands, and four in France. All those charged are males—seven of

them minors, the youngest age 16. To date, the only conviction is that of a 17-year-old British boy who pled guilty to arson not endangering life.

A clear difference exists in how authorities are charging these suspects. Most notably, Dutch prosecutors have levied charges such as causing an explosion, arson, and attempted **arson with terrorist intent** (<https://dutchbrief.com/four-suspects-in-rotterdam-synagogue-attack-formally-charged-with-terrorism/>). Similarly, suspects tied to a foiled improvised explosive device attack against a Bank of America office in Paris were charged with “**criminal terrorist conspiracy** (https://www.lemonde.fr/en/france/article/2026/04/07/the-strange-foiled-attack-on-bank-of-america-in-paris-he-said-if-the-kids-pulled-off-the-job-there-would-be-many-more_6752178_7.html)” and “attempted destruction in connection with a terrorist enterprise.” In other words, Dutch and French authorities have treated these cases as ideologically motivated terrorist acts with plausible indications of recruitment or external links. By contrast, British authorities have primarily charged suspects with standard arson and criminal damage offenses, even though all of the London incidents are being investigated by the Metropolitan Police Service’s Counter Terrorism Command due to the clear targeting pattern, ideological motive, and external claims.

Strategic Analysis

HAYI’s activities exemplify a classic proxy-style hybrid harassment operation, leveraging IRGC-style tactics to exert sustained, deniable pressure on governments and Jewish communities in Europe. Its rapid emergence, operational tempo, low-tech methods, and focus on symbolic targets reflect a deliberate strategy of calibrated attrition. The goal is to instill fear, provoke communal anxiety, strain security resources, and generate propaganda effects on Telegram and other channels, all while avoiding thresholds that would provoke unified Western retaliation.

As described above, HAYI’s model relies on opportunistic recruitment of disposable local operatives—predominantly young males with limited capabilities sourced through low-payment online channels or criminal networks. This decentralized “plug-and-play” approach minimizes logistical demands and risks for HAYI’s sponsors. Rather than pointing to potential false-flag operations intended to discredit Tehran, the pattern so far aligns closely with the established IRGC playbook for hybrid warfare. The consistent coordination and amplification of HAYI attack claims by seasoned hybrid warfare operators linked to Iran make repeated manipulation implausible.

Moreover, HAYI’s lack of the traditional hallmarks of terrorist organizations—such as training camps, formal propaganda arms, and hardened operatives—does not diminish the front group’s significance. Rather, it signals more brazen and extensive use of Tehran’s established approach to asymmetric warfare: namely, state-sponsored, low-profile, expendable proxies that prioritize deniability, scalability, psychological persistence, and volume over spectacular mass-casualty attacks.

HAYI thus serves as a lighter, more flexible instrument in Tehran’s proxy arsenal, complementing heavier actors like Hezbollah and forcing counterterrorism agencies to stretch resources across numerous low-sophistication incidents. Of course, the IRGC and Iran’s Ministry of Intelligence are not breaking new ground here. They have a **well-documented pattern** (<https://www.washingtoninstitute.org/iranexternalops/>) of outsourcing operations to criminal groups, teens, and other local actors, especially in Europe. For example, Iran has been tied to Hells Angels members charged with synagogue fire bombings and shootings in Germany in 2022; to various low-damage but highly symbolic attacks conducted in Sweden and Belgium by the gangs Foxtrot and Rumba; and to criminals involved in hostile reconnaissance and violence targeting opposition media in the UK.

The challenges posed by HAYI’s model are further highlighted by Europe’s differing legal responses, with some authorities applying terrorism frameworks and others relying on standard criminal damage charges. This illustrates

how a low-sophistication proxy campaign can complicate both attribution and effective responses.

In sum, HAYI's efficient design positions it to become a more persistent, widespread feature of the hybrid threat landscape. The front's ongoing activities underscore the growing difficulties that Western counterterrorism authorities face in addressing deniable, adaptive harassment campaigns amid unresolved geopolitical tensions.

Recommendations

As of this writing, the HAYI campaign remains active and has shown signs of possible escalation. Its evolution in the coming weeks will determine whether it serves as a limited-scope Iranian retaliation tool confined to Europe or a template for expanded deniable operations in the United States and elsewhere.

The campaign's persistence in Europe has already exposed critical vulnerabilities in government efforts to harden soft targets, curb online recruitment (particularly of minors), and protect Jewish communities amid spillover from Middle East conflicts. HAYI's operations generate widespread fear and divert resources at minimal cost to its Iranian sponsor. The campaign's effectiveness raises the risk of replication in the United States, where large Jewish communities, abundant soft targets, and similar recruitment vectors make for a highly attractive second theater. U.S. intelligence already noted an **elevated domestic threat level (<https://www.reuters.com/world/middle-east/intelligence-assessment-warns-iranian-attacks-us-following-khameneis-death-2026-03-02/>)** from Iranian proxies soon after the war broke out, and that assessment does not appear to have changed.

Given the broader counterterrorism challenge presented by HAYI's low-sophistication, high-volume approach, officials in the United States, Europe, and other jurisdictions should adopt a revised, proactive response model focusing on the following measures:

- **Strengthen resilience and community protection.** European officials should accelerate funding, security guidance, and physical hardening measures for Jewish educational and religious institutions and other soft targets. Likewise, American officials should proactively review and bolster protective measures for Jewish and Israeli-linked sites across the United States in anticipation of campaign spillover.
- **Disrupt recruitment and early-stage networks.** In general, the focus must shift to proactive disruption before attacks occur. Governments should therefore emphasize efforts to protect minors from online recruitment, with community organizations and specialized NGOs playing a key supporting role in implementation and outreach. At the same time, European intelligence and law enforcement agencies should enhance intelligence-led operations to map, infiltrate, and take down criminal intermediaries, facilitators, and online recruitment pipelines (especially on Telegram and Snapchat). In the UK, officials should take the additional step of formally designating the IRGC and its proxy networks as terrorist organizations. This would equip MI5 and the Metropolitan Police Counter Terrorism Command with the legal powers needed to shift from reactive low-level prosecutions of individuals to proactive dismantlement of networks.
- **Enhance attribution, intelligence sharing, and rapid response.** U.S. and European authorities should strengthen their forensic capabilities, expand and improve real-time intelligence-sharing mechanisms, and adopt more flexible, pattern-based attribution standards, which would enable faster operational responses and public exposure.
- **Impose costs on sponsors.** European governments have routinely issued diplomatic protests whenever Iran appears to foment violence on their soil (e.g., last week, London **formally summoned** (<https://www.gov.uk/government/news/summoning-of-the-iranian-ambassador-to-the-united-kingdom>) the Iranian ambassador after his embassy launched an online campaign calling for Iranians living in the UK to "Sacrifice for the Homeland"). Going forward, however, such protests should be coupled with more robust measures, including targeted sanctions, cyber and information operations to disrupt recruitment networks, selective diplomatic expulsions, and consistent public attribution.

- **Deplatform channels used for claims of responsibility.** Working with U.S. officials and major tech platforms, European governments should establish a dedicated rapid-response task force to monitor HAYI's propaganda ecosystem, identify claim videos through pattern-based attribution, and enforce removal within one hour of posting. The goal is to deny amplification and neutralize the group's primary propaganda tool.
- **Counter the psychological impact.** U.S. authorities, in coordination with European partners and Jewish community organizations, should take the lead on community reassurance messaging to reduce HAYI's attempts at fear amplification. Proactively bolstering protective measures for high-priority community sites would help in this regard.

Adrian Shtuni is the CEO of Shtuni Consulting LLC and an associate fellow with the International Centre for Counter-Terrorism. ❖

RECOMMENDED



ARTICLES & TESTIMONY

[The U.S. Shouldn't Lose Sight of the Real Terrorist Threats](#)

May 4, 2026

◆
Michael Jacobson

[\(/policy-analysis/us-shouldnt-lose-sight-real-terrorist-threats\)](#)



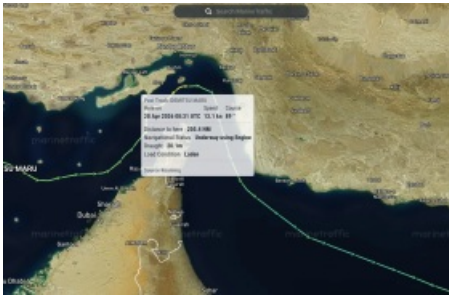
ARTICLES & TESTIMONY

[Is There a China Strategy Behind the Iran War?](#)

May 4, 2026

◆
Michael Sobolik,
Grant Rumley

[\(/policy-analysis/there-china-strategy-behind-iran-war\)](#)



BRIEF ANALYSIS

Why Iran's Navigational Order Will Be Difficult to Overturn

May 1, 2026



Noam Raydan

(/policy-analysis/why-irans-navigational-order-will-be-difficult-overtun)

TOPICS

Terrorism (/policy-analysis/terrorism)

REGIONS & COUNTRIES

Iran (/policy-analysis/iran)