

# TLP CLEAR – DISSEMINATION UNLIMITED



## In Obscura

Vincent M. Nasti, Founder, Chief Executive Officer, Consultant  
In Obscura, LLC | Threat Intelligence | Security Countermeasures | Investigations  
<https://inobscura.org/>

### (TLP-C) THREAT WARNING ISLAMIC CALL TO BOMB JEWISH TARGETS

3 APR 2026

KNOW THE TARGET – WATCH THE TARGET – LOOK DEEPER -EXPECT THE UNEXPECTED

**IN OBSCURA THEAT LEVEL – IMMINENT**

HOLY WEEK 2026 AND THE THREAT ENVIRONMENT SPIKES

---

CAVEAT: THIS INTELLIGENCE PRODUCT RELIES ON OPEN-SOURCE MEDIA OR GOVERNMENT RELEASED UNCLASSIFIED INFORMATION. RECOMMENDED ACTIONS ARE INCLUDED FOR CLIENTS FOR INFORMATION AND ACTIONS DEEMED APPROPRIATE.

---

#### PREDICATION

Among the OSINT sources I vetted and follow is Daniele Garofalo. I have cleared with him mu use of his products where appropriate. In his analysis below, I have added my own assessment in footnotes across the document. I respect his skill in analysis and have his approval to share his products to deliver to clients a comprehensive optic, reality of the threat to Christians, Clergy and Congregations.

In this unprecedented genocide and targeting of Christians. He uses the Bondi Beach attack as comparison and contrast. In Obscura has its own analysis on my website shortly after the attack, a potential second attack and tradecraft of the attackers. Yellow highlighted text AND Footnotes are mine.

###

#### Executive Intelligence Updates | Islamic State Call to Attack Jewish Targets

Immediate Threat Alert: Short-Term Operational Risk Assessment

Daniele Garofalo Apr 03, 2026

[https://www.danielegarofalomonitoring.com/p/executive-intelligence-updates-islamic?utm\\_source=post-email-title&publication\\_id=579565&post\\_id=193050211](https://www.danielegarofalomonitoring.com/p/executive-intelligence-updates-islamic?utm_source=post-email-title&publication_id=579565&post_id=193050211)

RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA

**TLP CLEAR – IN OBSCURA CAVEATS APPLY**

# TLP CLEAR – DISSEMINATION UNLIMITED

## Executive Intelligence Summary

Al-Naba Newspaper editorial no. 541 introduces a direct and time-bound call to action against synagogues and Jewish communities during Passover. The message is **not** descriptive but prescriptive, designed to activate individuals or micro-cells in the very short term. The call for the Bondi Beach stabbing attack December 2025 provides a replicable operational model, already validated in the jihadist narrative as an effective and low-cost action.

The screenshot shows a page from the newspaper 'Al-Naba'. At the top, it says 'بسم الله الرحمن الرحيم' (In the name of Allah, the Most Gracious, the Most Merciful) and 'العدد 541 الخميس 14 شوال 1447 هـ' (Issue 541, Thursday, 14 Shawal 1447 AH). The main headline is 'أقنابنا وأسرانا' (Our Masks and Our Captives). The text is in Arabic and discusses the situation in Iraq, mentioning the 'Al-Qaeda' group and the 'Islamic State' group. It calls for action against synagogues and Jewish communities during Passover. The page includes several images: a soldier in full combat gear, a Star of David, and a person in a white garment. The text is dense and appears to be a call to action.

The picture suggests a shift from ideological propaganda to immediate opportunistic mobilization, with a high probability of attempted attacks within the **April 3–9 window**, without the need for central coordination.

RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside information is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA

TLP CLEAR – IN OBSCURA CAVEATS APPLY

# TLP CLEAR – DISSEMINATION UNLIMITED

## Executive Risk Matrix

**Threat type:** inspired attacks, lone actor or micro-cell

**Likelihood:** high

**Impact:** medium to high

**Time horizon:** 0–7 days

**Geographic distribution:** global, concentration in Western urban contexts

**Primary targets:** synagogues, community centers, religious events

**Confidence Level:** moderate.

---

## Key Judgments

1. High probability of low-complexity attack attempts within 7 days
2. The dominant vector is the lone actor with simple weapons, knives, vehicles, and arson<sup>1</sup>
3. The narrative uses a real event to lower the threshold for action and normalize individual attacks
4. The narrow time frame indicates opportunistic intent, not a structured campaign
5. The main risk arises from the replicability and predictability of targets<sup>2</sup>.

---

## Strategic Risk Hierarchy

- Threat 1

---

<sup>1</sup> These weapons listed, and others are chosen for low price, tools and components in hand, the gathering of which by solo and micro operators is tradecraft, to nullify national security community outreach education on teaching indicators as in “see something, say something,” the detection of gathering supplies for instance, combined with neighborhood activity at a house like Santa Barbara will not exist.

<sup>2</sup> NOTE: In Obscura **myriad reporting and warnings concerning target surveillance and intelligence against churches across the US**, 99 percent of which were not and will not be detected. This cannot be emphasized stronger.

**RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA**

**TLP CLEAR – IN OBSCURA CAVEATS APPLY**

## TLP CLEAR – DISSEMINATION UNLIMITED

Attack with a knife, vehicle, or firearm against entrances or traffic areas of synagogues

- Threat 2

Arson or sabotage of community infrastructure

- Threat 3

Failed attempts with strong media coverage and subsequent imitation

---

### Threat Assessment

The threat level is high in the very short term. The operational capacity required is minimal and does not require advanced logistical support. The global distribution of targets, combined with the predictability of religious events, reduces complexity for the attacker.

**The risk lies not in sophistication, but in the potential frequency and difficulty of preventing isolated actors.**

---

### Operational Indicators

1. Increase in pro-IS content that revisits and reinterprets editorial 541
  2. Explicit references to Passover, religious vengeance, and the Gaza narrative
  - 3. Sharing rudimentary instructions for improvised attacks<sup>3</sup>**
  4. Online searches for times, locations, and access to places of worship.
- 

### Escalation Chain

- Phase 1
- 

<sup>3</sup> These instructions are commonly instructing on the aspiring attacker, gathering over the counter supplies which in their purchase are not alerting and then assembling parts to make an IED or avoid detection by security. The vehicle IED ramming attack in Meridian ID, was almost successful, in that SUBJECT bought multiple cans of gasoline, not reported to police and used a stolen medic into as the platform.

**RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA**

**TLP CLEAR – IN OBSCURA CAVEATS APPLY**

## TLP CLEAR – DISSEMINATION UNLIMITED

Editorial publication with a call to action

- Phase 2

Amplification in the pro-IS digital ecosystem

- Phase 3

Self-radicalization and identification with the message

- Phase 4

Individual mobilization and minimal planning

- Phase 5

Attack or attempted attack

- Phase 6

Media coverage and propaganda exploitation

- Phase 7

Copyright effect within 24–72 hours.

---

### Tripwires — Assessment of Changing Indicators

1. Successful attack in Europe or North America
2. Quick claim via Amaq News Agency
3. Dissemination of detailed operational instructions on closed platforms
4. Preventive arrests directly linked to al-Naba's call 541.

---

**RESTRICTED - PROPRIETARY INFORMATION.** The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA

**TLP CLEAR – IN OBSCURA CAVEATS APPLY**

# TLP CLEAR – DISSEMINATION UNLIMITED

## Early Warning Indicators

1. Surveillance activities near synagogues<sup>4</sup>
  2. Presence of isolated individuals exhibiting unusual behavior during religious events
  3. Increase in localized chatter in specific countries
  4. Reports of the purchase or preparation of incendiary materials.
- 

## Vulnerabilities

- Uncontrolled entrances or limited security
  - Predictable routines related to prayer times
  - Public events with high concentrations of people
  - Low perception of threat at the local level.
- 

## Cognitive Domain Assessment

- Target audience

Inactive sympathizers, marginalized individuals, and those already exposed to jihadist propaganda

- Cognitive triggers

Religious revenge, identity defense, polarization related to the Israeli-Palestinian conflict

- Activation pathway

Emotional stimulus → ideological legitimacy → simple operational model → individual action

---

<sup>4</sup> These are exceptionally important to become adept at detecting, which includes churches. Suspicious vehicle behavior, verbal and non-verbal behaviors of visitors, people you have not seen at church. Clothing not appropriate for the weather, backpacks, unattended items, unexpected packages especially those left at the door to the church. Odd phone calls, questions, same with email inquiries, odd statements in emails or receipt of US Mail with similar questionable statements or writings.

**RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA**

**TLP CLEAR – IN OBSCURA CAVEATS APPLY**

## TLP CLEAR – DISSEMINATION UNLIMITED

- Mobilization potential

High in the very short term, rapidly decaying without further stimulation

- Information effect
- Maximum propaganda yield even with low-lethality attacks.

---

### Key Intelligence Questions

Which channels are most amplifying Editorial 541?

Are there geographic clusters with a significant increase in online activity?

**Are there any signs of pre-operational surveillance?**

**Are there known individuals showing behavioral acceleration?**

---

### Intelligence Gaps

Actual number of individuals activated or in the process of being mobilized

Level of coordination between pro-IS channels

**Ability to transform the message into concrete action**

**Actual geographic distribution of risk.**

---

### Protective Posture Recommendations<sup>5</sup>

- Visible presence of security forces at sensitive targets
- Temporary access control during religious events
- Direct coordination with community security

---

<sup>5</sup> In Obscura considers these steps mandatory and especially vital to early indicator detection and denial of access to their target

**RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA**

**TLP CLEAR – IN OBSCURA CAVEATS APPLY**

## TLP CLEAR – DISSEMINATION UNLIMITED

- Activation of rapid reporting channels
  - Increased patrols in high-density urban areas
- 

### Implications for Decision-Makers

The critical window is immediate, with the initial 72 hours crucial

**Visible deterrence reduces the likelihood of opportunistic attacks**

The main risk remains unpredictable and decentralized

The response must be rapid, visible, and coordinated.

---

### Forecast 0–7 Days

- Most likely scenario

Isolated or failed attempts with high media coverage

- Alternative scenario

A successful attack in a Western urban context with rapid copycat effect

- Low probability scenario

Multiple uncoordinated but temporally close events.

---

### Confidence Assessment

**High confidence on intent and timing**

Moderate confidence on execution

Low confidence on scale and distribution of attacks.

---

**RESTRICTED - PROPRIETARY INFORMATION.** The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA

**TLP CLEAR – IN OBSCURA CAVEATS APPLY**

# TLP CLEAR – DISSEMINATION UNLIMITED

## Executive Intelligence Conclusion

The current threat environment is defined by a narrow and immediate activation window, **driven by direct incitement from Islamic State messaging aligned with a high-visibility<sup>6</sup>** religious event. The risk is not rooted in organisational capability, but in the speed and accessibility of individual mobilisation.

**The most credible threat scenario involves low-complexity attacks against exposed and predictable targets, particularly synagogues and community gatherings, where symbolic value and operational feasibility intersect.**

**Over the next 72 hours, deterrence posture and visible security measures will play a decisive role in reducing attack probability. The primary risk remains the unpredictability of self-activated individuals, operating without detectable coordination but within a clearly defined narrative and temporal framework.**

**Operational focus must remain on immediate protection, rapid information sharing, and early detection of behavioural anomalies. Delay in response directly increases exposure.**

---

## Executive Intelligence Cycle

This assessment is part of a broader analytical cycle.

*Founding subscribers receive the Executive Intelligence Briefing, which integrates all threat assessments, cognitive domain analysis, and a rolling 30–90 day forecast into a single monthly strategic synthesis.*

---

© Daniele Garofalo Monitoring - All rights reserved.///END///

---

<sup>6</sup> As we have seen each Holy Week or annual attack universities, as well with the fathwa or call for attacking Christian or Jewish property, congregations, businesses, reactive to an attack by friendly forces, the attack can be quick, unplanned yet not well executed and still be a victory in blood. It is absolutely vital that security forces be situationally aware, perpetually for indicators and most importantly, anomalies; that which isn't right, makes no sense but does not fit a definition of an indicator: expect the unexpected

**RESTRICTED - PROPRIETARY INFORMATION. The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA**

**TLP CLEAR – IN OBSCURA CAVEATS APPLY**

# TLP CLEAR – DISSEMINATION UNLIMITED


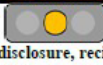


IN OBSCURA HAS ADOPTED THE OSINT CLASSIFICATION SYSTEM OF DHS DEPARTMENT OF HOMELAND SECURITY CLASSIFICATION: TLP CLEAR, TLP Clear: when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **HOWEVER IN OBSCURA RELEASE PROHIBITION MARKINGS APPLY** <https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usagg>

=====

**REQUEST WRITTEN PERMISSION, EMAIL, PRIOR TO DISSEMINATING ANY IN OBSCURA PRODUCTS OR INFORMATION.**

## TRAFFIC LIGHT PROTOCOL REQUIREMENTS FOR DISSEMINATION

### [Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
<p style="text-align: center;"><b>TLP:RED</b></p>  <p>For the eyes and ears of individual recipients only, no further disclosure.</p>	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved.	Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
<p style="text-align: center;"><b>TLP:AMBER</b></p>  <p>Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that <b>TLP:AMBER+STRICT</b> restricts sharing to the organization only.</p>	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.
<p style="text-align: center;"><b>TLP: GREEN</b></p>  <p>Limited disclosure, recipients can spread this within their community.</p>	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.
<p style="text-align: center;"><b>TLP: CLEAR</b></p>  <p>Recipients can spread this to the world, there is no limit on disclosure.</p>	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

///END OF REPORT///

**RESTRICTED - PROPRIETARY INFORMATION.** The information contained herein is for use by IN OBSCURA Clients and designated local, state, and federal, law enforcement and security agencies. Outside dissemination is prohibited. This document is the proprietary and intellectual property of IN OBSCURA, LLC. RESTRICTED FROM DISCLOSURE//NOT FOR PUBLIC RELEASE OR NEWS MEDIA

**TLP CLEAR – IN OBSCURA CAVEATS APPLY**