Soft Target Security Brief

Fortune Favors the Prepared | Intelligence Operations Division | Practitioner Edition

UNCLASSIFIED - OPEN SOURCE - FOR PUBLIC DISTRIBUTION

⚠ PREPAREDNESS CONDITION 4 - INCIDENT POSSIBLE ⚠

FIFA World Cup under way (opened 11-JUN Dallas; US opened 12-JUN LA) - soft targets outside stadiums are the dominant exposure. Iran kinetic track de-escalating: settlement announced 11-JUN (unsigned), modestly lowering direct-retaliation pressure, but the Iranian-proxy and lone-actor soft-target threat to Jewish institutions persists. Al-Saadi KH/HAYI: not-guilty plea 02-JUN, 8-count indictment, 09-SEP next date. NTAS under-managed since FEB 2026 funding lapse.

COMMUNICATIONS CONDITION: COMCON 4 - WATCH

World Cup under way adds ambient communications/GNSS load and an elevated cyber-fraud surface in host cities (ticketing, transport, hospitality). DHS flags drones as a top threat to large sporting events. Persian Gulf GNSS interference continues per MARAD advisory. No CONUS communications backbone failure.

WEATHER: WX-CON 3 - ENHANCED

SPC Day 1 SLIGHT today: damaging winds/isolated hail across the Appalachians, Mid-Atlantic, and Northeast (overlaps NE/Philadelphia World Cup venues this weekend). Day 2 ENHANCED eastern KS into west-central IL. See DTR Full Sec 7.

SPACE WEATHER: SWX-CON 2 - ACTIVE WATCH - G2 (Moderate) storm WATCH issued for 13-JUN

SWPC G2 (Moderate) geomagnetic storm WATCH issued for 13-JUN (WATA30). G1 reached K-index 5 on 11-JUN 2040 UTC. Coronal Hole 63 stream arrived. Minor HF/GNSS degradation possible at high latitudes.

SEASONAL: GRADUATION CLOSED - FIFA WORLD CUP UNDER WAY (OPENED 11 JUN)

Commencement season closed ~31 May. FIFA World Cup 2026 is UNDER WAY (opened 11 June in Dallas) as the dominant summer soft-target driver. US team opened 12 June in Los Angeles. 16 host cities across the US, Canada, and Mexico active for 39 days through 19 July; the key exposure is the soft-target environment outside the stadiums.

ISSUE PARAMETERS

Publication (UTC)	12 JUN 2026 / 1700 UTC
Reporting Period	08-JUN through 12-JUN 2026 (Issue 8 - Issue 9 window)
Issue	Vol. 1, Issue 9 | Supersedes Vol. 1, Issue 8 (08 Jun 2026)
SOP / Registry	SOP v5.57 | Master Source Registry v2.24 | ICD 203/206 per §0.113
NTAS Status	NO CURRENT ADVISORY - NTAS under-managed since FEB 2026 funding lapse; last bulletin expired SEP 2025

STANDING POSTURE - HOUSES OF WORSHIP / JEWISH INSTITUTIONS

The following mitigations remain in force from prior cycles regardless of whether a specific credible threat is identified this week:

- Vehicle standoff at all entrances - bollards, planters, or law-enforcement presence at drop-off points. A vehicle is the lowest-skill, highest-lethality tool available to a solo attacker.
- Child-area and youth-program access control - sign-in procedures, adult escort requirements, and staff-to-child ratios enforced at all times. The Al-Saadi indictment language included Jewish "schools" as a target category.
- HVAC intake audit - air intake locations mapped and access controlled. UK institutional hardening toward chemical-exposure kits signals UK CT assessment treats this vector as plausible.
- Mail and package intake protocol - all incoming packages screened before entering the interior. Train staff to identify IED precursor characteristics.
- FBI JTTF liaison - if your synagogue or JCC does not have an established FBI field office liaison, establish it now. Commissioner Tisch's statement that she has not seen a threat environment like this in

18 years of government was made at a synagogue security briefing - that briefing pipeline exists; access it.
• Nonprofit Security Grant Program (NSGP) FY2026 - ADL secured a $30M increase in NSGP funding for FY2026. Apply if you have not already done so. Funding covers physical security hardening, cameras, access control, and training.

BOTTOM LINE UP FRONT

Three things define your security calculus this cycle:
1. Al-Saadi pleaded NOT GUILTY on 02-JUN before U.S. District Judge Colleen McMahon in Manhattan. A formal 8-count indictment supersedes the original 6-count complaint. Next court date: September 9, 2026. The network he commanded remains distributed across Europe with cells at large. The threat the case represents is current and continuing.
2. FIFA World Cup 2026 is UNDER WAY (opened 11 June in Dallas; US team opened 12 June in Los Angeles). The tournament spans 16 host cities across the US, Canada, and Mexico over 39 days, running to 19 July. The dominant exposure is the soft-target environment OUTSIDE the stadiums - fan zones, watch parties, transport hubs, hospitality, and FanZones - which lack the rigid perimeters of the venues. DHS has flagged drones as one of the biggest threats to large sporting events. Iran-related matches carry the highest potential for politically motivated demonstrations and heightened security attention. A multi-tenant FIFA ticket-fraud and credential-harvesting operation is active (CloudSEK; 4,000-plus fraudulent World Cup domains). Recorded Future has not identified a significant terrorist or violent-extremist threat specific to the tournament, but assesses soft targets in major US metros face heightened VE risk, with Mexican host cities at the highest physical risk from TCOs.
3. The antisemitic-incident baseline remains the operative threat picture. ADL records at least 22 physical synagogue attacks in the US over the past decade (about 80 worldwide as of June 2026), and the ADL Center on Extremism counts 21 antisemitic terror plots/attacks since January 2020, 13 of them in the past 20 months. Two new institution-targeting incidents this window: Congregation Albert Synagogue and the JCC in Albuquerque, NM (02-JUN, doors smashed, children evacuated per protocol), and a second vandalism in two weeks at Chabad of Guelph, Ontario (09-JUN). The 12-MAR Temple Israel (West Bloomfield, MI) vehicle-ram - where staff evacuated preschoolers and Jewish leaders credited preparation for the outcome - remains the clearest recent demonstration that the standing mitigations below save lives. Note: no current NTAS advisory is in force; the NTAS site has been under-managed since a February 2026 funding lapse and the June 2025 bulletin expired September 2025.
SOURCES: DOJ/SDNY (Al-Saadi 8-count indictment; not-guilty plea 02-JUN) - DOJ SDNY | Recorded Future / Rozin Security / Securitas (World Cup soft-target and cyber threat) - Recorded Future | CloudSEK (FIFA ticket-fraud operation) - CloudSEK | ADL (decade of synagogue attacks; threat-environment) - ADL | DHS/HSToday (NTAS under-management) - HSToday

CURRENT ACTIVE THREATS - 12 JUN 2026

STSB-001 | KH-HAYI US network: Al-Saadi pleads not guilty; 8-count indictment. **FLASH | CONTINUED | 27**

SALUTE

SIZE: One named senior KH commander in federal custody SDNY. Plot scope: simultaneous attacks on a Manhattan synagogue plus Jewish centers in Los Angeles and Scottsdale AZ. Network scope: 20-plus attacks across Europe and Canada. Parent FTO Kata'ib Hizballah: 7,000-10,000 members, 150-plus attacks on US forces since October 2023.

ACTIVITY: 02-JUN: Al-Saadi arraigned, pleaded NOT GUILTY before U.S. District Judge Colleen McMahon. 8-count indictment supersedes 6-count complaint. Defense: political prisoner and prisoner of war framing. Prosecutors: warned case may widen. September 9 next court date. Indictment details: April 30, 2026 final US-directed contact before detention; FaceTime real-time attack direction including a London synagogue attack call; $3,000 cryptocurrency down payment for synagogue bombing; $10,000 total offered.

LOCATION: Manhattan federal court (SDNY) - arraignment 02-JUN. Metropolitan Detention Center, Brooklyn - defendant held without bail. Collateral at-large cells: Amsterdam, Paris, London, Skopje - tied to HAYI/KH network per SDNY complaint. US target set named in indictment: Manhattan synagogue (specific target confirmed with synagogue leadership per NYPD), Jewish centers Los Angeles CA and Scottsdale AZ.

TIME: Complaint unsealed 15-MAY-2026. Indictment unsealed approximately 29-MAY through 02-JUN 2026 window. Arraignment 02-JUN 2026. Next court date: September 9, 2026. Original attack planning window: approximately April 2026. Defendant detained abroad 01-MAY-2026; transferred to FBI custody 14-MAY-2026.

EQUIPMENT: $3,000 cryptocurrency down payment for synagogue bombing; $10,000 total offered. Methods discussed: IED or arson for US targets. European attack methods: accelerant arson

	(gasoline and fireworks), IED, edged weapons, vehicle. Al-Saadi electronic devices seized by FBI on transfer; contain evidence of attack planning, coordination, and promotion per DOJ indictment. **UNIT:** FBI New York JTTF (lead arrest); SDNY prosecutors (Jay Clayton, US Attorney); NYPD (Commissioner Tisch public statement); DOJ National Security Division. Defense: attorney Andrew Dalack (political prisoner framing). Defendant: Mohammad Baqer Saad Dawood Al-Saadi, 32, Iraqi national, senior KH commander.
Why This Cycle	The not-guilty plea and 8-count indictment are the primary legal development this cycle. The case is now formally in the contested-litigation track; defense counsel has publicly framed the defendant as a political prisoner and prisoner of war, a narrative designed to delegitimize the prosecution. Prosecutors counter that Al-Saadi waived Miranda rights and made voluntary statements en route to the US, described his Soleimani-era travel companion relationship, and provided evidence of his IRGC and Kata'ib Hizballah coordination role on electronic devices. The network he commanded conducted 20-plus attacks across Europe and Canada. The US cell was disrupted pre-attack; the broader network was not.
Analyst Assessment	**DELTA THIS CYCLE** **CHANGED:** Al-Saadi arraigned 02-JUN before U.S. District Judge Colleen McMahon. Pleaded NOT GUILTY through an Arabic interpreter, declared himself a prisoner of war. Court cut him off. Case proceeds. **CHANGED:** 8-count indictment unsealed, superseding the original 6-count complaint. New counts detail the full European attack campaign direction, FaceTime real-time attack coordination, and April 30, 2026 final US-directed contact before detention. **CHANGED:** Next court date: September 9, 2026. Prosecutors warned the case could widen to more suspects. **NO CHANGE:** KH/HAYI European cells remain distributed and at large. No new HAYI claim identified in open source this cycle. UK arson cycle continues (see STSB-002). **ADDED:** CONTEXT: the Iran kinetic track is de-escalating - a settlement to end the war was announced 11-JUN (unsigned, unverified). This modestly lowers state-directed retaliation pressure, but does NOT retire the proxy/lone-actor soft-target threat: the HAYI network is distributed, ideologically self-sustaining, and the Al-Saadi case shows intent and capability already established independent of any ceasefire. **LIKELIHOOD:** A further KH/HAYI-linked attempt against a US Jewish or pro-Israel soft target over the next 60 days - roughly even chance. **CONFIDENCE:** MODERATE. **SUPPORTING ANALYSIS:** Network demonstrated intent, funding, and sustained European operational tempo since February 2026. The arrest disrupted the most advanced known US cell and raised operational risk, but a distributed multi-country network does not shut down from a single arrest. Defense narrative may be designed to signal continued operation to network members. The September 9 trial date creates a calendar pressure point - any network response to defend or avenge the defendant is a tripwire. Collateral European cells remain active and at large. **CHANGE FROM PRIOR:** PRIOR (Issue 6, 29-MAY): Defendant in pretrial custody; 6-count complaint; defense mounting political prisoner narrative. CURRENT (Issue 7, 08-JUN): NOT GUILTY PLEA ENTERED; 8-count indictment supersedes complaint; arraignment 02-JUN; September 9 next date; prosecutors warn case may widen. Likelihood unchanged at roughly even chance - arrest contained the most advanced US cell but the network structure is intact. **TRIPWIRES:** (1) Any new HAYI claim or KH-attributed attack in Europe, Canada, or the US this cycle; (2) Identification or arrest of a second US-based cell beyond Al-Saadi; (3) A change in Al-Saadi custody or bail posture; (4) An Iranian state statement endorsing retaliation against US targets specifically; (5) September 9 court date developments; (6) Any network response timed to the arraignment date or trial calendar. **COLLECTION GAPS** • Identity and location of US-based cells beyond Al-Saadi - not established in open source. • Whether Al-Saadi has cooperated with FBI under his Miranda waiver - not disclosed; cooperation would be the highest-value intelligence gap in the case. • Current HAYI operational leadership succession after Al-Saadi's detention - not established in open source.

	• Whether the named Manhattan synagogue target was specifically secured or whether reconnaissance of alternative US targets occurred post-arrest - NYPD confirmed working with the named synagogue but broader reconnaissance scope not established.
ALT HYP	**ALT A: The network attempts another US or Western soft-target attack within the near term despite the arrest. [roughly even chance]** INDETERMINATE - intent and capability established; no new US attempt confirmed this cycle; Whitechapel UK attack (STSB-002) confirms European network tempo continuing. ✓ **Supporting Evidence:** Documented 20-plus attack European/Canada campaign; demonstrated funding and tradecraft; active parent FTO with thousands of members; ongoing Iran conflict providing motivation; distributed network resilient to single-node arrest; no observable suppression of European tempo this cycle. ✕ **Ruling-Out Evidence:** The most advanced known US cell was disrupted pre-attack; arrest raises operational risk; elevated FBI/JTTF surveillance in the wake of the case; no new HAYI claim identified this cycle; international law enforcement coordination demonstrated. **ALT B: The arrest and prosecution materially suppress near-term network activity against US targets. [unlikely]** NOT OBSERVED - no measurable suppression of European network activity this cycle; Whitechapel attack confirms continuation. ✓ **Supporting Evidence:** A high-value operator is in custody with his electronic devices seized; international law enforcement coordination demonstrated across multiple countries; elevated surveillance and disruption pressure; Miranda waiver statements may compromise network OPSEC. ✕ **Ruling-Out Evidence:** Network is distributed and continued operating after prior European arrests; Iranian proxy tasking runs on its own timeline independent of individual operator arrests; the parent FTO is large and resilient; defense narrative signals continued political framing to network members.
SOURCES	DOJ/SDNY: 8-count indictment | Courthouse News: not-guilty arraignment 02-JUN | Kurdistan 24: arraignment defiant statement | CBS NY: NYPD Tisch statement | Prism News: not-guilty plea; case may widen | AP, NBC News, HSToday, DOJ SDNY complaint and indictment

STSB-002 | UK/Europe KH-HAYI arson: Whitechapel attack; UK SEVERE sustained.	**FLASH | UPDATED | 23**
SALUTE	**SIZE:** UK national threat level SEVERE. Approximately 30-plus people arrested in the London-area Jewish-site arson campaign; 8 charged; one 17-year-old guilty plea. Active arson cycle now confirmed in: Golders Green (Hatzola ambulances, March), Finchley, Kenton, Tower Hamlets, and Whitechapel (this cycle). European HAYI claims lodged across Belgium, France, Germany, Netherlands, North Macedonia since February 2026. **ACTIVITY:** This cycle: Arson attack on former synagogue, Whitechapel, East London. Counter Terrorism Policing London investigating; Commander Helen Flanagan confirmed CT is considering links to the broader pattern. Prior cycle highlights: Tower Hamlets defendant reported in court to have been in contact with an Iraqi phone number before the fire - hardening Iran-direction linkage. UK synagogues reportedly stocking chemical-exposure and bleeding-control kits - UK institutional response to CT assessment of mass-casualty escalation risk. **LOCATION:** Greater London: Whitechapel (this cycle), Tower Hamlets, Finchley, Kenton, Golders Green. European nodes: Amsterdam (Bank of New York Mellon firebombing), Paris (Bank of America attempt), London (multiple), Skopje, Belgium, Germany, Netherlands, North Macedonia. All tied to the single KH/HAYI network per SDNY Al-Saadi indictment. **TIME:** Arson-and-arrest cycle running continuously since late March 2026. Whitechapel attack: this cycle (30-MAY through 08-JUN). UK SEVERE threat level: no expiration date set. Campaign is

	assessed to be one operational stage ahead of the US, where the Al-Saadi cell was disrupted at the planning stage. **EQUIPMENT:** Accelerant arson (gasoline and firework devices confirmed per SDNY complaint); edged weapons (London stabbing of two Jewish men including a dual US-British citizen, 29-APR); vehicles. UK institutional hardening toward chemical-exposure (HVAC) and mass-bleeding response kits indicates UK CT assessment treats a chemical or mass-casualty escalation on a Western soft target as plausible within the current threat window. **UNIT:** Counter Terrorism Policing London (lead, Commander Helen Flanagan). Metropolitan Police. Same network as Al-Saadi US case per SDNY complaint. "Thugs for hire" local criminal proxy tradecraft per UK police characterization of IRGC methodology. US institutions: read UK posture as forward indicator of their own threat surface.
Why This Cycle	The Whitechapel attack is the fourth or fifth distinct London borough targeted in the HAYI-claimed arson campaign (prior: Golders Green Hatzola ambulances, Finchley, Kenton, Tower Hamlets). East London adds a new geographic vector - Whitechapel is a different community profile from the north-London Jewish residential areas previously targeted, indicating the network is expanding its geographic scope or using different local proxies. Counter Terrorism Policing London continues to lead, and the Met has characterized this campaign as the most intensive community operations the force has ever run. The UK posture - synagogues stocking chemical-exposure and bleeding-control kits - signals UK CT assessment treats a mass-casualty escalation as plausible. US institutions should read UK posture as a forward indicator.
Analyst Assessment	**DELTA THIS CYCLE** **CHANGED:** New arson attack on a former synagogue in Whitechapel, East London, investigated by Counter Terrorism Policing London this cycle (30-MAY through 08-JUN). Adds to the ongoing multi-borough arson pattern. **NO CHANGE:** UK national threat level: SEVERE. No change. **NO CHANGE:** Total UK arrest count approximately 30-plus (8 charged, 1 guilty plea per Issue 6). No new public count issued this cycle - treat as the operative figure pending a fresh Met Police statement. **NO CHANGE:** The Al-Saadi SDNY indictment continues to name this European network as the same operation, one stage further along than the US cell. **LIKELIHOOD:** Continued HAYI/KH-linked soft-target activity in Europe over the next 30 days - very likely. **CONFIDENCE:** HIGH. **SUPPORTING ANALYSIS:** Continuous arson-and-arrest cycle since March; the Whitechapel attack this cycle confirms the campaign did not pause after the Al-Saadi arrest. Distributed multi-country network with local criminal proxies; hard to fully suppress. UK SEVERE threat level sustained. **LIKELIHOOD:** An equivalent network-linked executed attack on US soil within the next 30 days - unlikely. **CONFIDENCE:** MODERATE. **SUPPORTING ANALYSIS:** The known US cell was disrupted pre-attack; elevated FBI/JTTF surveillance; no second US cell identified in open source. However, the Al-Saadi indictment warns case may widen; network intent toward US targets is established. **CHANGE FROM PRIOR:** PRIOR (Issue 8): Whitechapel East London arson added a new borough to the pattern. CURRENT (Issue 9): no new UK HAYI attack confirmed in open source this window; UK threat level remains SEVERE; the European arson campaign is assessed continuing. European likelihood maintained at very likely. US likelihood unchanged at unlikely with MODERATE confidence. **TRIPWIRES:** (1) A chemical or mass-casualty escalation in the European campaign - UK institutions pre-positioning for this; (2) A new HAYI claim or KH-linked attack on US soil; (3) Identification of a US-based cell beyond Al-Saadi; (4) A UK threat-level change (SEVERE to CRITICAL); (5) An Iranian state endorsement of the campaign; (6) Attack on a US or Western target during the FIFA World Cup window. **COLLECTION GAPS** • Current total UK arrest count and charge status for the Whitechapel attack specifically - not released in open source this cycle. • Whether any HAYI claims were lodged in Europe during the 06-JUN through 08-JUN window - no claims identified in open source but this gap is unverified; operator should check SCN and FBI JTTF liaison.

	• Identity and network position of the "Iraqi phone number" contact identified in Tower Hamlets court proceedings - not established publicly.
ALT HYP	**ALT A: The European arson and attack campaign continues at or above its current tempo over the next 30 days. [very likely]** OBSERVED IN PROGRESS - Whitechapel attack this cycle confirms the campaign is active. ✓ **Supporting Evidence:** Continuous cycle since March with no observed pause; Whitechapel attack this cycle post-Al-Saadi arrest demonstrates no suppression; distributed network using local criminal proxies; UK SEVERE level sustained; Iranian proxy tasking driving the campaign. ✕ **Ruling-Out Evidence:** Sustained UK CT arrests are degrading the network; heavy multi-country law enforcement attention; possible network caution after Al-Saadi arrest exposed some tradecraft and device contents to FBI. **ALT B: An equivalent network-linked executed attack occurs on US soil in the next 30 days. [unlikely]** INDETERMINATE - US intent demonstrated and confirmed in indictment; no executed US attack from this network has occurred. ✓ **Supporting Evidence:** Same network demonstrated US intent (Al-Saadi indictment); parent FTO large and resilient; Iran conflict provides sustained motivation; September 9 trial date creates a potential calendar pressure point. ✕ **Ruling-Out Evidence:** The known US cell was disrupted pre-attack; elevated FBI surveillance in wake of arrest; Al-Saadi Miranda waiver may have compromised network OPSEC; no second US cell confirmed in open source.
SOURCES	ITV News London: Whitechapel CT investigation | ITV News London: Kenton synagogue arson | Reuters/AP: UK ambulance arson arrests | SDNY Al-Saadi complaint (network linkage) - British Brief: CT police launch most intensive community operations ever

STSB-003 | World Cup under way. Fan zones / transport hubs the key exposure. Ticket-fraud live.	**FLASH | UPDATED | 21**
SALUTE	**SIZE:** 48 teams, 104 matches, 39 days across 16 host cities (11 US, 3 Mexico, 2 Canada). US venues: NY/NJ final (MetLife, 19 July), semifinals Dallas and Atlanta, plus Miami, Los Angeles, Boston, Philadelphia, San Francisco, Seattle, Houston, Kansas City. Aggregate US attendance in the millions. Fan zones and unticketed gathering areas outside secured stadium perimeters are the higher-exposure surface - stadium-scale crowds without stadium-scale screening. **ACTIVITY:** No specific credible physical attack threat to the tournament known in open source. Active multi-tenant ticket-fraud operation (CloudSEK): typosquatted domains, admin panel admin-zone[.]tbpay[.]uk, FIFA clones, admin logins 3-5 JUN; 4,000-plus fraudulent World Cup domains. DHS flags drones as a top threat. Tournament opened 11-JUN (Dallas); US opened 12-JUN (Los Angeles). Group stage to 27 June; final 19 July. **LOCATION:** 11 US host city metros simultaneously in scope for 39 days. Highest-risk surfaces: fan zones and unticketed gathering areas outside secured perimeters; transit hubs; hotels. No water bottles permitted inside stadiums. Counter-UAS zones active around venues. Houses of worship and Jewish institutions in host cities inherit elevated ambient risk during the window as collateral high-symbolism targets per the standing KH/HAYI threat picture. **TIME:** Tournament window: 11 June - 19 July 2026. Opens in 6 days. US team opens 12 June in Los Angeles. Threat tempo historically rises around marquee fixtures and in the days before them. The cyber fraud campaign is active NOW - pre-event is the highest-risk credential-compromise window. **EQUIPMENT:** Federal preparedness: $625 million venue security across 11 US host cities; $250 million FEMA counter-UAS to 11 host states. 400-plus law enforcement agencies coordinating. Historical attacker tool set for mass events: vehicles, firearms, IEDs. Cyber attack surface: ticketing systems, stadium operations, broadcast infrastructure, transit networks, hospitality platforms. Counter-

	UAS (detect/identify/track/mitigate) deployed; hostile drones remain assessed as paramount concern by federal planners. **UNIT:** Per-venue local law enforcement coordinating with DHS, CISA, FBI, FEMA for counter-UAS. Cross-border coordination with Mexican and Canadian authorities. FBI and security researchers (Fortinet FortiGuard Labs, Canadian Centre for Cyber Security) on cyber fraud campaign. Private venue operators and fan-zone organizers carry primary site-security responsibility per CISA guidance. Fans attending: no reusable water bottles inside any stadium per new security rule.
Why This Cycle	The tournament is now in-event. No specific credible attack threat to the tournament is known in open source, which is consistent with effective prevention and with Recorded Future's assessment. The structural concern is the soft-target environment OUTSIDE the secured stadium perimeters - fan zones, watch parties, transport hubs, hospitality, and FanZones across 16 cities for 39 days - which lacks stadium-scale screening. Ticket-fraud and credential-harvesting are live now; organizations with World Cup exposure should treat phishing and ticketing fraud as current operational threats. The Iran de-escalation modestly lowers state-directed pressure, but Iran-affiliated cyber actors remain a named risk to ticketing/transport/hospitality, and the KH/HAYI targeting logic ("Jews" and "those who support America and Israel") still fits a high-symbolism US event. Iran-related matches are the highest demonstration flashpoint.
Analyst Assessment	**DELTA THIS CYCLE** **CHANGED:** Tournament UNDER WAY: opened 11-JUN in Dallas; US team opened 12-JUN in Los Angeles. The threat environment is now in-event. 16 host cities (US/Canada/Mexico) over 39 days to 19 July. DHS flags drones as a top threat to large sporting events. **ADDED:** Multi-tenant FIFA ticket-fraud operation active (CloudSEK TRIAD): typosquatted domains, a commercial admin panel at admin-zone[.]tbpay[.]uk, high-fidelity FIFA clones; admin logins recorded 3-5 JUN; 4,000-plus fraudulent World Cup domains. Iran-affiliated cyber actors are a named risk to ticketing, transport, and hospitality systems. **NO CHANGE:** Canadian Centre for Cyber Security cyber threat bulletin (03-JUN-2026) assessment stands: the World Cup will almost certainly be targeted by cybercriminals, non-state actors, and state-sponsored actors across physical and digital infrastructure. **NO CHANGE:** Federal security investment unchanged: $625 million venue security across 11 US host cities; $250 million FEMA counter-UAS to 11 host states. 400-plus law enforcement agencies coordinating. **LIKELIHOOD:** A mass-casualty attack specifically at a World Cup stadium or its secured perimeter - unlikely. **CONFIDENCE:** MODERATE. **SUPPORTING ANALYSIS:** Scale of federal security investment ($625M venue, $250M counter-UAS); no specific credible threat known in open source; intensive federal-local-international coordination; hardened screened perimeters. MODERATE rather than HIGH confidence because the in-event threat picture spans 39 days and 16 cities and is not yet fully resolved. **LIKELIHOOD:** An attack in the broader US soft-target space during the 39-day tournament window - roughly even chance. **CONFIDENCE:** MODERATE. **SUPPORTING ANALYSIS:** Consistent with the historical pattern of elevated targeting around high-profile summer events. The KH/HAYI network has demonstrated explicit US targeting intent; the World Cup in 11 US cities provides a sustained high-profile target environment. DVE interest in large gatherings is a standing concern per CISA and DHS-FBI guidance. **LIKELIHOOD:** A significant credential-compromise or financial-fraud cyber incident tied to the active FIFA fraud campaign - likely. **CONFIDENCE:** MODERATE. **SUPPORTING ANALYSIS:** 4,000-plus fraudulent World Cup domains and a multi-tenant ticket-fraud admin operation are already live per CloudSEK; the risk is realized now, not future. MODERATE confidence reflects uncertainty about organizational-level vs individual-level impact. **CHANGE FROM PRIOR:** PRIOR (Issue 8): tournament imminent; ticket-fraud campaign confirmed active; physical threat picture with no specific credible threat. CURRENT (Issue 9): tournament UNDER WAY (opened 11-JUN); exposure shifts to soft targets outside stadiums; ticket-fraud operation detailed (CloudSEK); Iran de-escalation modestly lowers state-directed pressure while proxy/cyber risk persists. Physical likelihood unchanged; cyber-fraud likelihood remains likely.

TRIPWIRES: (1) Any DHS/FBI joint intelligence bulletin naming the World Cup as a specific target; (2) Any disrupted plot or claimed threat against a host city or fan zone; (3) A UAS incursion at any host venue; (4) An attack at any large summer gathering that serves as a template; (5) An Iran-track deterioration that raises FTO-inspired threat during the window; (6) Al-Saadi network activity timed to the World Cup opening.

COLLECTION GAPS

• 2026 pre-event DHS/FBI joint intelligence bulletin to law enforcement for summer mass-gathering events - the historical pattern is to issue this bulletin; it has not been confirmed issued this cycle, and the NTAS system under-management may have affected the advisory pipeline.

• Whether any specific credible threat intelligence against a World Cup host city or fan zone is held at classified channels not available in open source.

• Whether FEMA counter-UAS grants have been fully obligated and systems deployed at all 11 US host city venues as of opening week.

ALT HYP

ALT A: A successful mass-casualty attack occurs at a World Cup stadium or within its secured perimeter during the 39-day window. [unlikely]

INDETERMINATE - in-event; no specific threat reporting in open source this window.

✓ **Supporting Evidence:** Internationally symbolic target; sustained FTO and DVE interest in sporting events and large gatherings; very large crowds; 39-day window across 11 US metros; KH/HAYI network demonstrated US intent against targets in several host cities (NYC, LA).

✕ **Ruling-Out Evidence:** $625M dedicated venue security plus $250M counter-UAS; 400-plus law enforcement agencies; hardened screened stadium perimeters; no specific credible threat known as of opening week.

ALT B: If an attack occurs in the tournament window, it strikes a softer affiliated target (fan zone, transit hub, hotel, nearby gathering) rather than the secured stadium perimeter. [roughly even chance]

INDETERMINATE - the softer-target displacement pattern is documented in historical mass-event attacks; unrealized this window.

✓ **Supporting Evidence:** CISA assesses lightly secured accessible venues as the attractive target; fan zones carry stadium-scale crowds without stadium screening; historical mass-event attacks (Manchester Arena, Nice promenade) hit the perimeter and approach rather than the hardened venue interior.

✕ **Ruling-Out Evidence:** Federal security posture and FEMA funding extend to fan-zone and transit security in host cities, not just stadium interiors; heightened posture spans the entire host-city footprint.

SOURCES

J&Y Law: World Cup security on the ground - June 2026 | Canadian Centre for Cyber Security: cyber threat bulletin 03-JUN-2026 | The Hacker News: FIFA fraud campaign active | Paladin Risk Solutions: World Cup threat landscape | Security Magazine, TechFinitive, Fortinet FortiGuard Labs: FIFA cyber threat report

CONTEXTUAL BASELINE - ANTISEMITIC THREAT ENVIRONMENT

ADL 2025 Audit of Antisemitic Incidents - Released 06-MAY-2026

This audit was released after the prior STSB issue and constitutes the current operative baseline for the standing synagogue, JCC, and Jewish-institution threat picture. Key findings:

• 6,274 total antisemitic incidents in 2025 - average 17 per day. 33% decrease from 2024 but the third-highest year since ADL began tracking in 1979; five times higher than a decade ago.

• 203 physical assaults - the highest assault count ADL has ever recorded. Up 4% from 2024.

• 32 assaults involving a deadly weapon - up 39% from 23 in 2024.

• Three people killed in antisemitic attacks in 2025 - first antisemitic murder year since 2019. Incidents: Capital Jewish Museum shooting DC (two Israeli Embassy staffers), Boulder CO Molotov attack (Run for Their Lives event, one killed), Pennsylvania Governor Shapiro residence firebombing.
• 1,129 antisemitic incidents targeted Jewish institutions specifically in 2025.
• ADL secured a $30M increase in federal Nonprofit Security Grant Program (NSGP) funding for FY2026. Jewish institutions that have not applied for NSGP funding should do so.
• Companion legislation: Jewish American Security Act introduced in Senate (Senators Rosen and Lankford) 19-MAY-2026. Monitor for Congressional action.
NTAS STATUS NOTE: No current NTAS advisory is in force. The NTAS website has been under-managed since a February 2026 funding lapse per HSToday reporting. The June 22, 2025 bulletin (Iran conflict / heightened threat environment, expires September 22, 2025) is the last advisory in the public record. The absence of an NTAS advisory does not indicate the threat environment has normalized; it indicates the public-facing advisory system has not been updated in the current conflict environment. Operators should not use NTAS silence as a green indicator.
SOURCES: ADL 2025 Audit of Antisemitic Incidents (06-MAY-2026) - ADL: Jewish American Security Act welcome - HSToday: NTAS under-management - JTA, Jewish Insider, CBS New York: ADL audit coverage

SOURCING & STANDARDS

This issue was built against Master Source Registry v2.24 (629 sources suite-wide; 56 mandatory; STSB-tagged subset per registry v2.24). Mandatory STSB-relevant sources swept for the 08-JUN through 12-JUN window. Analytic judgments follow ICD 203/206 per SOP 0.113. Likelihood ladder: almost no chance, very unlikely, unlikely, roughly even chance, likely, very likely, almost certain. Confidence: HIGH, MODERATE, or LOW. Both stated separately on every judgment. Each scored card carries two alternative hypotheses with supporting and disconfirming evidence; changed judgments carry CHANGE FROM PRIOR. Sources: ADL, SPLC, Secure Community Network, SITE Intel, Counter Extremism Project, GNET, DHS/NTAS, FBI, CISA, Reuters, ACLED, CDC HAN, FEMA IPAWS, NWS, State Dept, COMCON/PREP-CON, and 46 additional STSB-tagged sources.
Mandatory source sweep summary: DHS/NTAS - no current advisory (under-managed since FEB 2026 funding lapse; last bulletin expired SEP 2025). FBI Public Advisories - World Cup ticket-fraud warning active; no new joint soft-target bulletin identified. CISA Advisories, Commercial Facilities, Government Facilities - no new soft-target bulletin this cycle; standing guidance current. Reuters / ACLED - Iran settlement announced 11-JUN (unsigned); no new CONUS STSB-relevant attack event. ADL - two institution-targeting incidents this window (Albuquerque 02-JUN; Guelph ON 09-JUN). State Dept - no new STSB-relevant travel advisory. CDC HAN - no new mass-casualty health alert. FEMA IPAWS / NWS - SPC Slight (NE) today; no STSB-relevant emergency alert. COMCON/PREP-CON - PREP-CON 4 Incident Possible (de-escalation from prior-cycle PREP-CON 3).
Gaps acknowledged: (1) DHS/FBI pre-summer mass-gathering joint intelligence bulletin: the historical pattern is to issue this bulletin before the summer event season; it has not been confirmed issued in 2026, and the NTAS system under-management may have affected the advisory pipeline - treat as an unresolved gap. (2) UK HAYI arrest count: prior cycle figure (approximately 30/8/1) is the most current available; a new Met Police public release was not identified this cycle. (3) HAYI European claims in the 06-JUN through 08-JUN window: no claims found in open source; unverified - operator should check SCN and FBI JTTF liaison. (4) Second US cell beyond Al-Saadi: not established; the highest-priority gap for this threat track.

CALENDAR HORIZON - NEXT 60 DAYS

Key dates for STSB tracking:
• Through 19 JUL 2026: FIFA World Cup in progress (opened 11 JUN Dallas; US opened 12 JUN LA). 16 host cities; group stage to 27 JUN; final 19 JUL. Soft targets outside stadiums are the standing exposure for the duration.
• 19 JUL 2026: World Cup Final, MetLife Stadium, NY/NJ. Highest symbolic value target of the summer.
• 09 SEP 2026: Al-Saadi next court date, SDNY. Monitor for any network response timed to this date.
• Summer window: Elevated DVE and FTO-inspired targeting probability. CISA/FBI historical pattern of summer event-season joint bulletins. No 2026 bulletin confirmed issued as of this cycle.

ANALYTICAL STANDARDS & SOURCING

This product is produced in conformance with ICD 203 (Analytic Standards) and ICD 206 (Sourcing Requirements). Likelihood and confidence are stated as separate dimensions on every forward-looking judgment. Likelihood uses the estimative ladder (almost no chance, very unlikely, unlikely, roughly even chance, likely, very likely, almost certain); confidence is HIGH, MODERATE, or LOW. Every scored entry carries a minimum of two alternative hypotheses with supporting and disconfirming evidence.

Analytical standards: fortunefavorstheprepared.com/analytical-standards **|** **Source registry:** fortunefavorstheprepared.com/dtr-source-registry