WEEKLY INTELLIGENCE ASSESSMENT

PERIOD: 2026-06-28 — 2026-07-05 · CLASSIFICATION: OPEN SOURCE

SIGNAL INTELLIGENCE SUMMARY

DOMAIN	SIGNALS	CRITICAL	HIGH	MODERATE	LOW	AVG SCORE
Counter-Terrorism	47	0	0	28	19	5.6
Cybersecurity	38	0	2	17	19	4.9
National Security Threats	95	0	1	57	37	5.0
Regional Conflicts	87	0	0	47	40	5.2
TOTAL	**267**	**0**	**3**	**149**	**115**	

WEEKLY INTELLIGENCE ASSESSMENT

Period: 28 June – 5 July 2026

Classification: For Analytical Use

EXECUTIVE SUMMARY

- [HIGH] The assassination of Iranian Supreme Leader Ali Khamenei — confirmed by state funeral rites in Tehran drawing mass mobilisation and the surfacing of IRGC Gen. Ahmad Vahidi after months in hiding — is the single most consequential threat vector this week. It has simultaneously activated succession-security concerns (Mojtaba Khamenei barred from the funeral on assassination grounds), Iranian proxy posturing in Lebanon and Syria, and Kurdish-IRGC clashes in western Iran, indicating regime instability is now the primary driver of Middle East risk rather than any single conflict theatre.
- [HIGH] The most significant actor movement is the convergence of US-Pakistan re-alignment with India's hardening counter-terror posture: MHA designation of 17 Pakistan-based individuals plus 23 UAPA terrorist designations, Indian air defence procurement (₹52,000 Cr) and MAPSS drone induction, and Indian rhetoric on the Indus Waters Treaty all track against US backing of "Pakistan's right to self-defence" at the UN. This is not routine friction — it is a structural realignment of the South Asian security architecture.
- [MODERATE] Highest-confidence prediction: Russian pressure on Ukraine will intensify through mid-July via aerial bombing (Sumy strike, Kostiantynivka claims) and expanded drone operations into Europe from "shadow ships," while Russian

domestic fuel shortages create an incentive for Putin to seek battlefield signalling rather than negotiation before the NATO Ankara summit.

- [MODERATE] Most important emerging signal: state-linked cyber actors (Armored Likho targeting government/power sector; China-linked actors expanding beyond tech targets) are shifting toward AI-enabled operations concurrent with Trump's AI cybersecurity executive order and CIA's AI overhaul — indicating the AI-cyber competitive cycle has entered an operational, not aspirational, phase.

STRATEGIC SYNTHESIS

1. Converging Threats. Four developments are causally linked this week. First, Khamenei's assassination and funeral (national security) is directly generating regional conflict spillover: IRGC ambushes against Kurdish fighters in western Iran, Druze–Syrian government clashes, and Lebanese President Aoun's public plea for continued US backing all reflect a proxy network recalibrating under leadership shock. Second, reporting that US officials believed Israel planned to kill Iranian negotiators during peace talks — if accurate — establishes a causal chain from the Israeli decapitation campaign to the current UN warning of "risk of miscalculation" in the Strait of Hormuz. Third, the India–Pakistan counter-terror escalation is being enabled by permissive US signalling on Pakistan while simultaneously being contested by US politicians pushing to delist Syria as state sponsor of terrorism — a broader pattern of Washington loosening designations that historically disciplined state behaviour. Fourth, cyber and AI developments (Trump's AI EO, CIA's AI overhaul, China-linked actor expansion) are not standalone — they are the technical infrastructure layer beneath the US–China "new Great Game" in the Middle East explicitly identified in this week's reporting.

2. Shared Actors & Infrastructure. Iran operates across all four domains simultaneously: national security (leadership succession), regional conflict (Lebanon/Syria/Kurdish theatres), counter-terrorism (Vahidi's re-emergence signals IRGC-Quds Force continuity), and — by extension through proxies — cyber posture toward Gulf targets. Russia similarly spans domains: kinetic operations in Ukraine, drone campaigns into European airspace launched from maritime "shadow" platforms, and continued state-aligned cyber activity (Armored Likho against government and power-sector targets fits established GRU/FSB tasking patterns). China's cross-domain footprint is quieter but structural: expanded cyber targeting beyond tech sectors, the Taiwan blockade scenario reporting, and the Beijing–Dalai Lama succession dispute all reflect a single strategic posture on legitimacy and territorial control. Pakistan-based militant designations and Karachi/KP operational activity (two police killed in Mohmand) demonstrate that state-tolerated non-state actors remain the core dual-use capability in South Asia.

3. Compound Risk Scenarios.

Rank 1 (probability MODERATE, impact HIGH): An Iranian succession crisis triggers an IRGC-led escalation in the Strait of Hormuz or Lebanon concurrent with a Russian-manufactured incident on NATO's eastern flank ahead of the Ankara summit. This would force the US into two-theatre crisis management with degraded bandwidth for South Asia, allowing Pakistan-based groups a permissive window and India a rationale for

kinetic response. Indicator convergence is already present: UN "miscalculation" warning, Merz's Baltic tour, and Indian air defence acceleration.

Rank 2 (probability LOW–MODERATE, impact HIGH): A state-linked cyber intrusion into Western critical infrastructure (power sector via Armored Likho-class TTPs or the new Avalon/CrownX ransomware framework) coinciding with a Taiwan Strait provocation. The Bad Epoll Linux kernel flaw and MSSQL initial-access research indicate the vulnerability surface is currently expanding faster than defensive posture, and China-linked actors are demonstrably broadening target sets.

4. Strategic Blind Spots. The assumption warranting the strongest challenge: that Khamenei's death produces a *managed* succession. Reporting shows Mojtaba Khamenei was barred from his father's funeral due to assassination concerns and Vahidi surfaced only for the ceremony — both indicate the security apparatus does not trust its own operational environment. The IC is likely underweighting the probability of an internal IRGC power struggle producing autonomous proxy action *without* Tehran central authorisation, particularly in Lebanon and Iraq. A second blind spot: the AI-cyber threat discussion is being framed as US–China competition, but the Avalon/CrownX and PamStealer developments indicate criminal frameworks are absorbing AI-enabled capabilities on a shorter timeline than state actors, creating an under-attributed threat vector.

DOMAIN ASSESSMENTS

CYBERSECURITY

Active actors: Armored Likho (Russia-aligned, targeting government agencies and power sector with BusySnake stealer); China-linked actors expanding beyond technology sector targets; criminal operators deploying the new Avalon framework (with integrated CrownX ransomware) and PamStealer macOS credential theft tool.

TTPs: Initial access via MSSQL exploitation and fake free-software lures deploying RATs; abuse of in-game logic to hijack AI browser sessions without user typing (novel credential exfiltration path); exploitation of Bad Epoll Linux kernel flaw enabling unprivileged root escalation, with Android exposure.

Sectors targeted: Government, energy/power, macOS enterprise users, satellite ground infrastructure (ST Engineering iDirect iQ-Series terminals and CubeSpace CW0057 reaction wheel advisories indicate space-segment exposure).

Cross-domain flag: Armored Likho power-sector targeting aligns temporally with Russian kinetic pressure on Ukrainian energy infrastructure — analytic judgment: coordinated hybrid campaign, MODERATE confidence.

COUNTER-TERRORISM

Key actors: Pakistan-based groups (17 individuals designated by MHA; 23 UAPA designations); TTP-affiliated elements active in KP (Mohmand police attack); Palestine Action (UK proscription contested); residual concerns over Syrian jihadist re-legitimisation via proposed delisting.

Operational patterns: Continued cross-border militancy against Indian and Pakistani state targets; ideological contestation in Western universities over proscribed

groups; Indian emphasis at UN on AI in counter-terrorism signals capability rather than doctrinal shift.

Geographic spread: Concentrated South Asia (India-Pakistan-Kashmir), with secondary UK ideological dimension and Syria policy debate in Washington.

Cross-domain flag: Turkish "strategic triad" gaining Trump-administration sway complicates Israeli counter-terror operational latitude and may constrain intelligence-sharing on Hamas/Hezbollah — direct link to regional conflict domain.

REGIONAL CONFLICTS

Active zones: Southern Lebanon (Israel-Hezbollah framework judged inadequate); Gaza (Hamas internal execution for alleged Israeli collaboration indicates counter-intelligence pressure); Syria (Druze-government clashes); western Iran (IRGC-Kurdish); Ukraine (Sumy, Donetsk, Kostiantynivka); Sudan (al-Obeid humanitarian catastrophe).

Escalation indicators: UN warning on Hormuz miscalculation; alleged Israeli plan to kill Iranian negotiators; Russian drone launches from maritime platforms into Europe.

De-escalation indicators: Limited — Israel-Lebanon framework exists but is assessed non-reassuring by regional actors.

Cross-domain flag: The "new Great Game" US-China Middle East dynamic creates a permissive environment for cyber and proxy actors as major powers hedge commitments.

NATIONAL SECURITY

State-level threats: Iranian leadership succession under active security threat; Russian sustained war effort despite domestic fuel shortages; India's ₹52,000 Cr air defence acceleration and indigenous drone induction.

Intelligence operations: CIA AI overhaul under Ratcliffe signals doctrinal shift toward machine-speed collection and analysis.

Geopolitical shifts: US-Pakistan warming assessed by regional analysts as strategically costly; NATO cohesion strained ahead of Ankara summit (Merz-Trump friction over spending).

Cross-domain enabler flag: The CIA AI overhaul and Trump AI EO together establish federal architecture that will shape cyber, counter-terror, and conflict domains for the remainder of the administration.

EMERGING THREATS

- **[Cybersecurity]** — AI browser session hijacking via in-game logic manipulation (six AI browsers demonstrated vulnerable without user keystroke input). Confidence: **MODERATE**. Why it matters now: this is the first credible operational demonstration that agentic AI browsers can be weaponised as a credential-theft vector at scale, bypassing traditional phishing detection.
- **[National Security]** — Iranian post-Khamenei succession security paranoia (Mojtaba barred from funeral; Vahidi's controlled re-emergence). Confidence: **HIGH**. Why it matters now: indicates the IRGC assesses ongoing decapitation risk from Israeli

intelligence, which raises the probability of pre-emptive proxy escalation as a deterrence signal.

- **[Regional Conflicts]** — Russian drone launches from maritime "shadow" vessels into European airspace. Confidence: **MODERATE**. Why it matters now: extends the Ukraine war's kinetic geography into NATO territory via deniable platforms, complicating Article 5 thresholds ahead of the Ankara summit.

PREDICTIVE ASSESSMENT — 7 TO 14 DAY OUTLOOK

- [HIGH] — Iran will name a successor or transitional leadership council within 14 days, with IRGC influence over the selection exceeding clerical influence. **Trigger indicator:** Assembly of Experts convening announcement or IRGC senior officer public prominence at state events.
- [HIGH] — Russia will conduct at least one major aerial strike against a Ukrainian urban centre (Kyiv, Kharkiv, or Sumy) timed within 72 hours of the NATO Ankara summit. **Trigger indicator:** Iskander/Kalibr movement to launch positions; Shahed swarm assembly reports.
- [MODERATE] — India will conduct additional UAPA designations or a limited kinetic operation against Pakistan-based infrastructure within 14 days. **Trigger indicator:** MEA statement invoking Indus Waters Treaty; forward deployment of Indian Air Force assets to western bases.
- [MODERATE] — A state-linked cyber intrusion targeting European or US energy-sector operator will be publicly disclosed, with TTPs consistent with Armored Likho or successor toolset. **Trigger indicator:** CISA or ENISA advisory referencing BusySnake or MSSQL initial-access chains.
- [MODERATE] — Hezbollah will conduct a limited kinetic signal against Israeli positions in southern Lebanon to demonstrate post-Khamenei operational continuity. **Trigger indicator:** Aoun public statement on Israeli overflight; UNIFIL incident reporting.
- [LOW-MODERATE] — A Strait of Hormuz maritime incident (tanker interference, GPS spoofing, or boarding) will occur, driven by IRGC signalling rather than central Tehran authorisation. **Trigger indicator:** UKMTO advisory; unusual IRGCN small-boat sortie patterns from Bandar Abbas.

KEY ACTORS & ENTITIES

ACTOR	TYPE	PRIMARY DOMAIN	CROSS-DOMAIN ACTIVITY	CURRENT POSTURE	THREAT TRAJECTORY
IRGC / Gen. Ahmad Vahidi	State security apparatus	National Security	Regional conflict (Lebanon, Syria, Kurdish clashes); proxy CT	Succession-defensive, operationally active	↑
Russian Federation (Kremlin/GRU)	State	Regional Conflicts	Cyber (Armored Likho power-sector); drone ops into Europe; energy warfare	Kinetic escalation despite domestic strain	↑
People's Republic of China	State	National Security	Cyber espionage expansion; Taiwan blockade planning; Tibet succession	Preparatory posture, non-kinetic	→
Government of India (MHA/MoD)	State	Counter-Terrorism	Air defence acquisition; AI-CT at UN; Indus Waters signalling	Assertive, hardening	↑
Pakistan-based designated militants	Non-state	Counter-Terrorism	KP operational activity; India-facing plotting	Sustained tempo	→
Hezbollah	Non-state armed group	Regional Conflicts	Iranian proxy signalling post-Khamenei	Restrained, testing framework	↑
Israel (IDF/Mossad)	State	Regional Conflicts	Alleged decapitation ops against Iranian negotiators; Lebanon posture	Offensive-forward	↑
Hamas	Non-state armed group	Regional Conflicts	Internal CI operations (Gazan execution); Gaza military posture	Defensive-attritional	→
Armored Likho	State-aligned APT	Cybersecurity	Power-sector targeting supporting Russian kinetic goals	Active campaign	↑

ACTOR	TYPE	PRIMARY DOMAIN	CROSS-DOMAIN ACTIVITY	CURRENT POSTURE	THREAT TRAJECTORY
Turkey (Erdogan gov't)	State	Regional Conflicts	"Strategic triad" influence on US ME policy; NATO summit host	Rising influence broker	↑
Trump Administration (US)	State	National Security	AI EO; CIA overhaul; Pakistan re-alignment; NATO friction	Restructuring alliances	↑
Kurdish armed groups (western Iran)	Non-state armed group	Regional Conflicts	Direct IRGC engagement	Under pressure, reactive	→

End of Assessment.

Analytic judgments reflect evidence available in the reporting period. Reassessment required upon Iranian succession announcement or NATO Ankara summit outcomes.