ExpertView
CAPSS
CENTRE FOR AEROSPACE POWER AND STRATEGIC STUDIES
27/26

AI at War: What OSINT, AI, and the Iran Conflict Teach India

Air Vice Marshal Prashant Mohan VM (Retd)
Additional Director General, CAPSS

14 September, 2026

Keywords: Artificial Intelligence, Open-Source Intelligence (OSINT), AI-Enabled Targeting, Iran–Israel Conflict, Indian Defence Modernisation.

Israel and the United States fought two Iran wars within the span of a year, and both were shaped by the same underlying factor: open-source intelligence, fused with artificial intelligence, turned into operational effect. The first, in June 2025, was Israel's Operation Rising Lion and America's Operation Midnight Hammer, a twelve-day campaign against Iran's nuclear infrastructure and military leadership that ended in a ceasefire around June 24-25.[1] The second, Operation Epic Fury for Washington and Operation Roaring Lion for Tel Aviv —began on February 28, 2026 and has continued to shape the region in particular and the world in general.[2] Together, these two campaigns describe one continuous arc of Artificial Intelligence (AI)-enabled Open-Source Intelligence (OSINT) preparation, execution, and retaliation, rather than two unrelated events joined only by geography. For India, this fusion of open-source collection and artificial intelligence offers considerably more instruction than either war would on its own.

Where AI-Enabled OSINT Fits into the Targeting Effort

Israeli intelligence officers have described, on the record, how AI shaped the June 2025 campaign's targeting. One officer explained that AI was used to “sift through troves of data” collected over years, sorting potential targets into leadership, military, civilian, and infrastructure categories, then filtering for individuals closely tied to the Islamic Revolutionary Guard Corps (IRGC).[3] That sorting function is what earlier generations of analysts did by hand, slowly, and often only for the handful of targets that mattered most. AI allowed the same discipline to be applied across a far larger dataset without a proportional increase in analyst hours. Human intelligence supplied the raw material; AI then organised it. Mossad's former research director has described agents compiling dossiers on Iranian

commanders that included where they worked and where they spent their free time, and stationing weapons near Iranian air-defence sites years in advance.[4] That fusion of pattern-of-life detail and machine sorting is what let Israel strike Revolutionary Guard commander Hossein Salami, armed forces chief Mohammad Bagheri, and eight Guard members in a single bunker within the campaign's opening hours.[5]

By the 2026 phase, the same logic operated at greater speed and scale. The AI fused drone footage, satellite passes, and telemetry into targeting packages, enabling more than 1,000 discrete strikes inside Iran within Epic Fury's opening 24 hours.[6] Within days, an independent technologist had reconstructed a minute-by-minute replay of the campaign using AI agents to scrape open-source signals before they could be purged from digital caches, built entirely from public data—a civilian demonstration of the exact fusion the military had just carried out at classified scale.[7] Intelligence gathering, pattern-making and strike execution had become stages of one continuous, AI-mediated pipeline, rather than separate functions handed off between agencies with the delays that handoff usually implies.

A Long-Drawn Effort, not a Single Campaign

Neither strike came out of nowhere, and treating either as a discrete, fast-moving event misreads how it was actually built. Israeli officials have described the June 2025 operation as “the culmination of years of work,” built on roughly three years of dossier compilation, infiltration and pre-positioning of smuggled drones and weapons inside Iranian territory.[8] That preparation defined three distinguishable operational pillars, each running on its own timeline. Sustained human and technical collection came first and should be measured in years, not months. Forward pre-positioning by special operations followed, embedding the physical means to strike quickly once collection matured. Only at the final stage did AI-assisted integration turn the accumulated material into an executable targeting picture, and that stage was by far the fastest of the three.

The 2026 phase did not repeat this process from zero. It drew on the same intelligence base, redirected toward a renewed campaign once the 2025 ceasefire broke down. AI proportionally did more work in the fusion the second time round. The AI stage was the fastest part of the process and also the smallest, sitting atop years of unglamorous collection that no algorithm replaced or compressed. Speed at the point of decision should not be mistaken for speed across the whole effort. Technology procurement is the easy part on any realistic timeline, and the multi-year human-collection base underneath it is the part that actually determines whether the technology has anything useful to fuse.

What This Should Interest India About

An Indian defence commentator has already drawn out the operational implications directly from the June 2025 campaign, arguing that India should deepen intelligence-military synergy and move toward "actively employing assets for preemptive disruption" rather than treating intelligence gathering and strike planning as separate functions handled by separate institutions on separate timelines.[9] He also stresses accelerating indigenous drone and AI development, and recommends a unified Special Operations Command to coordinate covert intelligence with conventional forces, mirroring the IDF-Mossad relationship that made Rising Lion possible.[10] Both recommendations follow directly from the operational pillars described above. The capability that mattered most across both Iran campaigns was not any single AI tool, but the standing organisational bridge between collectors, analysts, and shooters that let AI's contribution reach the battlefield quickly when needed. India's own Operation *Sindoor* experience in May 2025 offers a partial domestic parallel worth weighing against this.

A second, less comfortable lesson concerns vendor dependence. Days after Claude's integration into Maven had reportedly helped enable the Epic Fury strikes, the Pentagon formally designated Anthropic a "supply chain risk," after the company declined to remove safeguards against mass surveillance and fully autonomous weapons use.[11] A federal judge later ruled that designation unlawful.[12] Whatever the merits of that specific dispute, it demonstrates something India should take seriously on its own account. A state's AI-OSINT capability can be only as reliable as its relationship with the company that built the underlying model, and that relationship can turn adversarial for reasons that have nothing to do with battlefield performance. India should weigh that dependency carefully.

Iran's Riposte and How Much of It Was OSINT

Iran's retaliatory missile and drone campaign, styled Operation True Promise IV, generated its own substantial open-source footprint. An independently maintained OSINT dataset has tracked the campaign in close to real time, logging waves against Israeli and coalition targets across a dozen countries, built entirely from open-source reporting rather than classified feeds.[13] That dataset says as much about the transparency of this particular war as about Iran's own tradecraft. It was built by an outside analyst observing Iran, not by Iran itself, and its existence shows how thoroughly this conflict has been documented by parties with no operational stake in either side. Iran's own use of OSINT was narrower and more targeted than the wide, crowd-verified tracking effort aimed at it.

It centred on monitoring US and allied force positions across the Gulf using commercially available satellite imagery, reportedly supplied in part by the Chinese firm Chang Guang Satellite Technology, which a Western think-tank report describes as collecting and supplying Iran with imagery of US and allied military facilities.[14] Iranian ground-based jamming and spoofing of GNSS signals across the Strait of Hormuz was a related but analytically distinct capability, electronic warfare rather than open-source collection. The two should not be conflated in any serious accounting even though both degraded the information environment for the other side simultaneously.[15] Iran-aligned regional partners added a further, less formal layer to this picture. Militia and proxy networks across the region have long supplied low-cost human observation of shipping and troop movements that supplements, and sometimes substitutes for, the satellite and signals collection a better-resourced state would otherwise need to build on its own. None of this amounted to an OSINT capability comparable in scale to what tracked Iran from the outside. It was narrower, more improvised, and built substantially on imported rather than indigenous tools, a pattern that recurs throughout Iran's information effort in this conflict.

Force Multiplier, Not Frontier Capability

Iran's own AI use, according to a detailed threat-intelligence assessment published in mid-2026, was real but modest in ambition, and the distinction matters for how the whole episode should be read. AI, the assessment concludes, "very likely accelerated existing Iranian capabilities across cyber, influence, military and domestic repression domains, rather than creating new ones."[16] The clearest documented examples were generative, not analytical. One Iran-aligned propaganda outlet used AI to produce a finished two-minute video, complete with an AI-generated rap song, in about 24 hours.[17] Iranian malware researchers appear to have used generative AI to help write code for at least one documented backdoor, leaving telltale artefacts, such as emoji embedded inside debug strings, that are rarely found in work written entirely by hand.[18] Iran's own claims of AI-enhanced drone guidance have not been independently confirmed during the conflict. The confirmed AI-enabled hardware, Nvidia-based modules recovered from Iranian-designed drones, had actually been documented in Russian use over Ukraine rather than over Iran, a detail that complicates any straightforward claim about Iranian AI-drone capability.[19]

Iran leaned heavily on outside supply to compensate for what it evidently could not build domestically. Russia reportedly agreed to supply AI-enabled drone hardware during the conflict itself, and Chinese surveillance technology, including deep-packet-inspection tools and camera systems from established Chinese vendors, underpinned Iran's domestic monitoring capability

throughout.[20] Where India might reasonably expect a peer adversary to eventually field frontier AI of its own, Iran instead demonstrated what a well-resourced but heavily sanctioned state can still achieve by applying comparatively modest AI gains to tools and to external partnerships it already had in place.

What India Should Take from Iran's Experience

The Iranian case offers a more encouraging lesson than the Israeli one, precisely because it required less to produce a real effect. A state does not need frontier AI to gain meaningful advantage. Applying AI as a force multiplier to existing malware, propaganda and drone programmes produced measurable operational and information effect even under sustained sanctions and export controls.[21] That is a realistic, resource-conscious target for India's own capability-building, distinct from and considerably more achievable than chasing Maven-scale ambition outright in the near term. The second lesson is more concrete and immediate, and it is already being made by Indian commentators rather than only inferred from abroad. India's own analysis of this conflict has flagged a specific navigational vulnerability. Barely three of India's eleven Navigation with Indian Constellation (NavIC) satellites are said to be fulfilling their core purpose, with at least one past its expected service life, even as Iranian jamming showed how quickly GNSS-dependent operations can be degraded by a determined, resource-limited adversary.[22] The same analysis recommends India develop encrypted, anti-jam, military-grade navigation signals and expand NavIC into a genuinely independent constellation. This, alongside domestic “drone farms” capable of producing the volumes of low-cost systems that Iran's own missile-and-drone campaign demonstrated still matter against far more expensive interceptor missiles.[23] Mass and resilience, in other words, remain as strategically relevant as sophistication. A third, quieter lesson follows from Iran's reliance on Chinese and Russian technology rather than domestic development. India's own neighbourhood already features exactly this kind of collusive technology transfer, and an adversary short on frontier capability but well supplied by a capable partner should be treated as a serious planning assumption, not a lesser threat simply because the underlying AI is borrowed rather than built at home.

Building India's Own AI-OSINT Capability

Four facets of this conflict deserve to shape how India builds its own capability. The first is organisational, not technical - the standing bridge between human collectors, open-source analysts and operational planners that both the Israeli and Iranian efforts depended on more than any single algorithm.[24] Quality control matters here as much as speed. A well-built OSINT-AI cell needs disciplined human-machine teaming and verification tradecraft precisely because AI can fuse bad

data into a confident-looking picture just as fast as it can fuse good data. The cost of that error only shows up after a decision has already been made.

The second facet is sovereignty over the AI layer itself. The Anthropic-Pentagon dispute shows that dependence on a foreign AI vendor is not a hypothetical risk confined to trade policy; it is a live operational one, capable of disrupting a capability at precisely the moment it matters most, for reasons entirely outside the user's control.[25] India's own commentators have already argued for reducing dependence on foreign AI vendors for both threat detection and verification tooling, a recommendation that applies with equal force to offensive OSINT-AI fusion and not only to defensive cybersecurity.[26]

The third facet is realistic scoping of ambition. Iran's experience shows that AI applied to existing tools, malware, propaganda, and geolocation can produce real effect without frontier capability or unrestricted compute access.[27] India does not need to match Maven's scale to gain meaningful advantage from this technology; it needs disciplined, well-resourced application of what it already has, which is a considerably more achievable near-term target than trying to out-compute far better-resourced states from a standing start.

The fourth facet is technical and specific rather than doctrinal: navigation resilience. An AI-OSINT capability that depends on GNSS-linked platforms, as most modern collection and strike systems now do, is only as strong as the signal underneath it. Iranian jamming over the Strait of Hormuz demonstrated how quickly that layer can be contested even by an adversary without a frontier AI programme of its own.[28] Hardening NavIC, and building the indigenous drone-production base to match it, are concrete, fundable engineering steps rather than open-ended aspirations, and both can proceed in parallel with the slower organisational and sovereignty work described above.

Institutional proposals already under discussion in India, including a hybrid civilian-military reserve force intended to provide surge capacity during a crisis, point toward the kind of standing capacity this fusion ultimately requires if it is to be more than a peacetime demonstration project.[29] None of these four facets is exotic, and none depends on a technological breakthrough India does not already have some purchase on. Each is a deliberate answer to something this particular conflict actually demonstrated, rather than a general aspiration to "have AI" in the abstract, and that distinction is the one India's own capability-building effort cannot afford to lose sight of as it moves from scoping to execution.

Notes:

[1] Jack Moore, "Israel and Iran Agree to Ceasefire to Bring End to '12 Day War,' Trump Says," *ABC News,* June 24, 2025, https://abcnews.com/International/israel-iran-agree-ceasefire-bring-end-12-day/story?id=123137697. Accessed on September 03, 2026.

[2] Adam Simmons, "The New Battlespace: How Geospatial AI Is Reshaping Military Intelligence," *Project Geospatial,* March 12, 2026, https://projectgeospatial.org/geospatial-frontiers/the-new-battlespace-how-geospatial-ai-is-reshaping-military-intelligence. Accessed on September 03, 2026.

[3] Julia Frankel and Sam Mednick, "How Israel Used Spies, Smuggled Drones and AI to Stun and Hobble Iran," *The Times of Israel,* June 17, 2025, https://www.timesofisrael.com/how-israel-used-spies-smuggled-drones-and-ai-to-stun-and-hobble-iran/. Accessed on September 03, 2026.

[4] Ibid.

[5] Ibid.

[6] Simmons, n. 2.

[7] "Mindblowing: Osint Expert Recreates Timeline of Operation Epic Fury in Interactive 3D Model," *J Feed*, March 02, 2026, https://www.jfeed.com/news-world/operation-epic-fury-3d-replay. Accessed on September 03, 2026.

[8] Frankel and Mednick, n. 3.

[9] Hemant Mahajan, "Lessons for India from the Israel-Iran Conflict: An Analysis of OP RISING LION," *Indus Research,* June 19, 2025, https://indusresearch.in/lessons-for-india-from-the-israel-iran-conflict-an-analysis-of-op-rising-lion/. Accessed on September 03, 2026.

[10] Ibid.

[11] "Pentagon Labels AI Company Anthropic a Supply Chain Risk," *NPR,* March 06, 2026, https://www.npr.org/2026/03/06/g-s1-112713/pentagon-labels-ai-company-anthropic-a-supply-chain-risk. Accessed on September 05, 2026.

[12] Ibid.

[13] Daniel Rosehill, "Iran-Israel War 2026 Data — OSINT Dataset," *Promise Denied Project,* https://danielrosehill.github.io/Iran-Israel-War-2026-OSINT-Data/. Accessed on September 05, 2026.

[14] Can Kasapoğlu, "The War Above the War: How Chinese Satellites Support Iran," *Hudson Institute,* May 29, 2026, https://www.hudson.org/national-security-defense/war-above-war-how-chinese-satellites-support-iran-mena-defense-can-kasapoglu. Accessed on September 05, 2026.

[15] Adithya M. Nair, "Strategic Lessons for India from the 2026 Iran War," *Indian Defence News,* June 14, 2026, https://www.indiandefensenews.in/2026/06/strategic-lessons-for-india-from-2026.html. Accessed on September 05, 2026.

[16] "AI Has Enhanced Iran's Asymmetric Playbook During the 2026 Conflict," *Recorded Future,* July 16, 2026, https://www.recordedfuture.com/research/iran-ai-asymmetric-playbook. Accessed on September 05, 2026.

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Nair, n. 15.

[23] Ibid.

[24] Frankel and Mednick, n. 3.

[25] NPR, n. 11.

[26] Sindhu Vissamsetti, "AI-Powered Espionage: How India's Cybersecurity Strategy Must Evolve," *CyberPeace Foundation,* November 29, 2025, https://cyberpeace.org/resources/blogs/ai-powered-espionage-how-indias-cybersecurity-strategy-must-evolve. Accessed on September 05, 2026.

[27] Recorded Future, n. 16.

[28] Nair, n .15.

[29] Sameer Dasaka, "Building India's National Cyber Reserve Force: Feasibility, Models, and Strategic Value," *Nat Strat,* August 21, 2026, https://www.natstrat.org/articledetail/publications/building-india-s-national-cyber-reserve-force-feasibility-models-and-strategic-value-284.html. Accessed on September 05, 2026.