TREADSTONE 71

STRATEGIC & CYBER INTELLIGENCE

AMERICANS IN THE CROSSHAIRS

Iranian Threats to Strike US and Allied Infrastructure in Europe

A Consolidated Finished Intelligence Assessment

Open-source, defensive threat intelligence · No operational content

Probability language: Sherman Kent half-open bands · Source grading: NATO Admiralty (6×6) · Evidence layer: ASA Tri-Score (T/D/F)

Contents

1. Bottom Line Up Front (BLUF)
2. Key Judgments
3. Situation: An Active War, a Decapitated Regime
4. The Closing Window: Bezmer Expires 1 October
5. The Rybar Product and the Influence Operation
6. Capability Assessment: Reach, Precision, Magazine
7. Target-Selection Logic and Taxonomy
8. Attack Vectors and Feasibility
9. Third-Party / Proxy Enablers (2026)
10. Named Units, Suppliers & Supply-Chain Interdiction
11. Economic Coercion: The Sharper Lever
12. Outlook: Scenarios and Cones of Plausibility
13. Structured Analytic Techniques
14. Evidence Layer: ASA Tri-Score and Admiralty
15. Intelligence Gaps and Collection Requirements
16. Recommendations
17. Caveats and Sourcing

Figures

Fig 1 Chronology of the 2026 war and the Europe thread
Fig 2 Bezmer authorization window (closing)
Fig 3 Rybar influence-operation network
Fig 4 Iranian delivery-system reach vs. named targets
Fig 5 Ballistic-missile stockpile: depletion and reconstitution
Fig 6 Attack-vector assessment matrix
Fig 7 Iran capability supply chain & interdiction
Fig 8 Hormuz economic shock, 2026
Fig 9 Near-term scenarios with Sherman Kent bands
Fig 10 Cones of plausibility
Fig 11 Execution roadmap (ranked, sequenced)
Fig 12 Deterrence asymmetry: Bezmer vs Akrotiri
Fig 13 Tanker displacement if Bezmer closes

1. Bottom Line Up Front (BLUF)

The Rybar product is a dual-purpose artifact. It is a factually anchored threat report wrapped in a Russian information operation. The pro-Kremlin channel Rybar (@rybar_mena) took genuine, independently reported facts and reframed them. Those facts are real: the 19 August 2026 Financial Times report, the Bezmer tanker deployment, and March's Akrotiri drone strike. The frame is not. It is built to widen NATO fracture anxieties. Two things are assessed here, the kinetic threat and the influence operation. The second matters more.

In the near term, a direct strike on Bezmer or Akrotiri is Unlikely (15 to <45). Deniable sub-threshold action is Likely (55 to <85). Iran can reach both bases on paper. Precision at European ranges is another matter, and untested. The launcher pool is severely depleted. A strike on alliance soil would also remove Iran's own off-ramp. So Tehran leans the other way. Its revealed preference, proven across the 2026 war, is calibrated, deniable, reversible escalation: proxy drones, shipping and cable coercion, cyber, and transnational repression.

This is happening inside an active war. The regime is decapitated and hardened, and it has foreign targeting help. This is not pre-war strategic-patience Iran. Supreme Leader Ali Khamenei was killed on 28 February 2026. Mojtaba, his hardline son, now leads. Iran has killed 18 US personnel and wounded about 760 (Pentagon, 21 August). Analysts tie its improving precision to Russian and Chinese support. The intent read moves with it, toward coercive signaling with a fatter miscalculation tail.

Update, 27 October 2026

Bezmer resolved itself before the vote this assessment expected. Both KC-135s, the only two of eight authorized, left Bulgaria on 21 August, the cut-off day, "to support other operational requirements." Sofia held no extension vote, and the authorization lapsed unused on 1 October. No official tied the departure to the FT report or to Iran. KJ-6 is overtaken. Where the tankers went is undisclosed, so the relocation call stays untested.

- **No Iranian or proxy strike has hit European or Cypriot soil since the cut-off. KJ-1, KJ-3 and the sub-threshold scenario hold.**
- **The economic war escalated. US strikes on Iran's Hormozgan coast resumed 1 to 4 September and continue periodically. Trump rejected Iran's seven-day Hormuz plan on 26 September. On 22 October the IRGC announced an "offensive" doctrine, and ship attacks and mines lifted Brent to about $117 on 23 to 24 October. KJ-5 holds; shipping attacks now run above the squeeze the scenarios assumed, while the cables remain untouched.**
- **Deniable action continued off the kinetic track. An IRGC-linked intrusion took a small UK power station offline for four days in July (reported 23 August). A Czech investigation on 21 September exposed Rybar crews filming across Europe.**
- **Hezbollah disarmament has not moved. Prime Minister Salam ties it to a full Israeli withdrawal, and Israel still holds ground in southern Lebanon.**
- **Watch item: on 24 October Trump said the US "may do another Epic Fury" after the 3 November midterms. A major new US campaign is the trigger this assessment names for a direct strike or a deniable proxy hit on an allied base.**

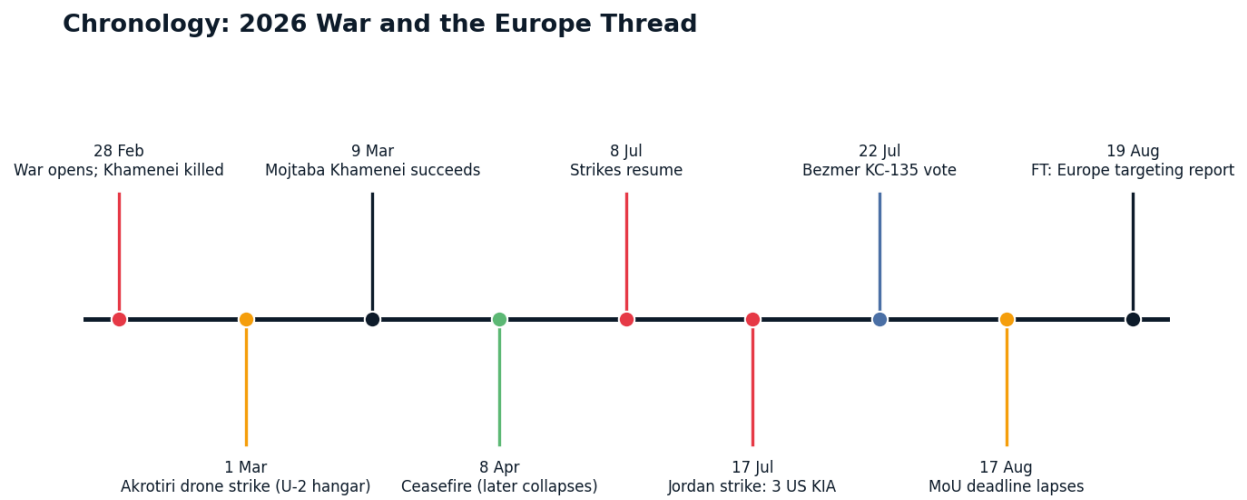
2. Key Judgments

- **KJ-1.** Iran holds a contingency assessment against European targets, not a confirmed strike order. Likely (55 to <85), on Admiralty B2 to B3 sourcing from two FT-sourced regime insiders. No target packages or launcher pre-positioning toward the Eastern Mediterranean are observed in open source.

- **KJ-2.** The most-likely channel is deniable and sub-threshold. Likely (55 to <85): proxy one-way-attack UAV against Cyprus-class targets, Hormuz cable and shipping coercion, cyber, and diaspora operations in Europe.
- **KJ-3.** A direct missile strike on alliance territory is Unlikely (15 to <45) near-term and self-deterring. The floor sits higher than a peacetime model would set, given the hardliner succession and improving, externally enabled precision.
- **KJ-4.** Rybar's amplification is the higher-probability, higher-yield operation. Its narrative payoff, splitting allied resolve and unsettling host publics, exceeds the kinetic payoff of a strike against heavily defended bases.
- **KJ-5.** Economic coercion is Iran's sharpest lever. Highly likely (85 to <95) it remains the primary pressure tool: the 2026 Hormuz shock drove Brent to an intraday high of $126 on 30 April and cut traffic to about 10 vessels a day.
- **KJ-6.** The Bezmer authorization expires 1 October 2026, 41 days from cut-off. A fresh Bulgarian parliamentary vote is required to continue. Likely (55 to <85) that the renewal fight, rather than any missile, dominates September, and that Russian information operations aim squarely at it.

3. Situation: An Active War, a Decapitated Regime

War came on 28 February 2026, when the US and Israel struck first in Operation Epic Fury. The opening blow was a decapitation that killed Supreme Leader Ali Khamenei and much of the senior command. His son **Mojtaba Khamenei**, assessed as more hardline, took the leadership on 9 March 2026. A Pakistan-brokered ceasefire followed on 8 April. It collapsed. Strikes resumed on 8 July. The 60-day memorandum-of-understanding deadline then lapsed on 17 August, the parties deadlocked over the Strait of Hormuz. A fragile pause now holds under a US naval blockade. Eighteen US service members are dead. About 760 are wounded (Pentagon, 21 August). The European targeting question sits inside this war, not beside it.



Underneath all of it sits the nuclear grievance. Two rounds of strikes hit the program. The 12-Day War of June 2025 struck Natanz, Fordow, and Isfahan; the 2026 campaign hit Natanz again, the SPND headquarters at Lavisan-2 / Mojdeh, and a covert site at Minzadehei. Damage assessments diverge sharply. Israel's Atomic Energy Commission called Fordow inoperable and the setback "many years." A leaked US Defense Intelligence Agency report judged the sites damaged but not destroyed, with centrifuges largely intact and a delay measured in months. CSIS notes that roughly 400 kg of 60 percent enriched uranium remains unaccounted for. IAEA inspectors have had no access to Fordow, Natanz or Isfahan since June 2025, and Iran's parliament suspended cooperation with the agency. The analytic point is not the setback figure. It is that a regime which believes its deterrent was destroyed, which operates without inspection, and which is

now led by a hardliner, carries structurally higher risk tolerance. The “no limits” rhetoric and the European targeting assessment are both downstream of that grievance.

Strain at home sharpens the tail. Iran runs this war inside an economic collapse. Inflation ran near 68 percent year on year in February 2026, the rial fell sharply, and the winter brought the largest protests since 1979. Mojtaba Khamenei has reshuffled toward IRGC hardliners; Mohsen Rezaei became Supreme National Security Council secretary on 9 August with his endorsement. A cornered regime under new hardline leadership carries both a diversionary-escalation incentive and thinner decision discipline. The direct-strike judgment stays Unlikely, but its floor sits nearer the top of that band during acute domestic crisis.

Figure 1. Chronology of the 2026 war and the Europe thread. Sources: Al Jazeera, CNN, NPR, CBS, Britannica, Wikipedia 2026-war article set (dates cross-checked).

4. The Closing Window: Bezmer Expires 1 October

Sofia's authorization is temporary. It runs out in 41 days. Bulgaria's parliament approved the deployment on 22 July 2026 by 136 votes to 13, with two abstentions, for the period 24 July to 1 October 2026 only. It covers up to eight KC-135 tankers and up to 250 personnel. Under the 2006 US–Bulgaria Defense Cooperation Agreement, Bezmer is a joint-use facility, and any continued presence needs a fresh parliamentary vote. The first two tankers landed on 31 July.

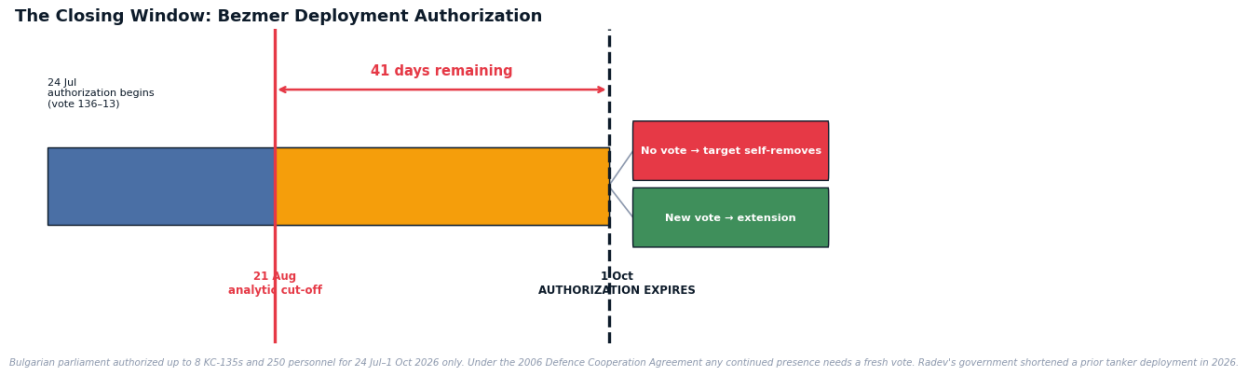


Figure 2. The Bezmer authorization window. Sources: BTA, Xinhua, Novinite, Army Recognition, Bulgarian National Assembly record (22 Jul 2026).

Sofia may remove the target without Tehran firing anything. The political ground is not solid. Prime Minister Rumen Radev's government has already shortened one US tanker deployment: tankers placed at Sofia Airport in February 2026 under the previous government, without parliamentary authorization, were given a 30 June end date and left by the end of that month. On the July vote, GERB-UDF, Democratic Bulgaria, and We Continue the Change all abstained from participating. The 13 votes against came from Vazrazhdane and one Progressive Bulgaria member. Mayors of five municipalities around the base issued a joint statement warning of added risk; residents of Bezmer village collected more than 500 signatures in under 24 hours and organized protests. Defense Minister Dimitar Stoyanov told parliament that no offensive weapon systems would sit on Bulgarian soil.

Three consequences follow. First, if Tehran is weighing action against these specific aircraft, it faces a countdown, and waiting costs it nothing. Second, the Rybar operation has a cheaper endpoint than a missile: make extension politically impossible in Sofia, and the tankers leave on their own. That outcome serves Moscow and Tehran better than a strike, and it carries none of the Article 5 risk. Third, PIR-1 gains urgency. Any real Iranian target package for Bezmer would have this date inside it. We assess it Likely (55 to <85) that the extension vote becomes the main contested ground through September, and Roughly even (45 to <55) that the deployment is extended in some form.

5. The Rybar Product and the Influence Operation

Rybar is a directed Russian information asset. It is not independent OSINT. The UK sanctioned Rybar and its principal Mikhail Zvinchuk on 9 December 2025. That designation treats it as a state-directed information actor that masquerades as an independent outlet, and the US Rewards for Justice offer of October 2024 ties it to Rostec funding. Ten Rybar staff followed on 13 July 2026. Watch what the product does. It launders a paywalled FT report to Russian-speaking and MENA audiences, then adds a persuasive "reachability" map. Then it hedges its own alarm (*"only propaganda effect," "could backfire"*). That hedge builds analyst trust while still seeding the core frame.

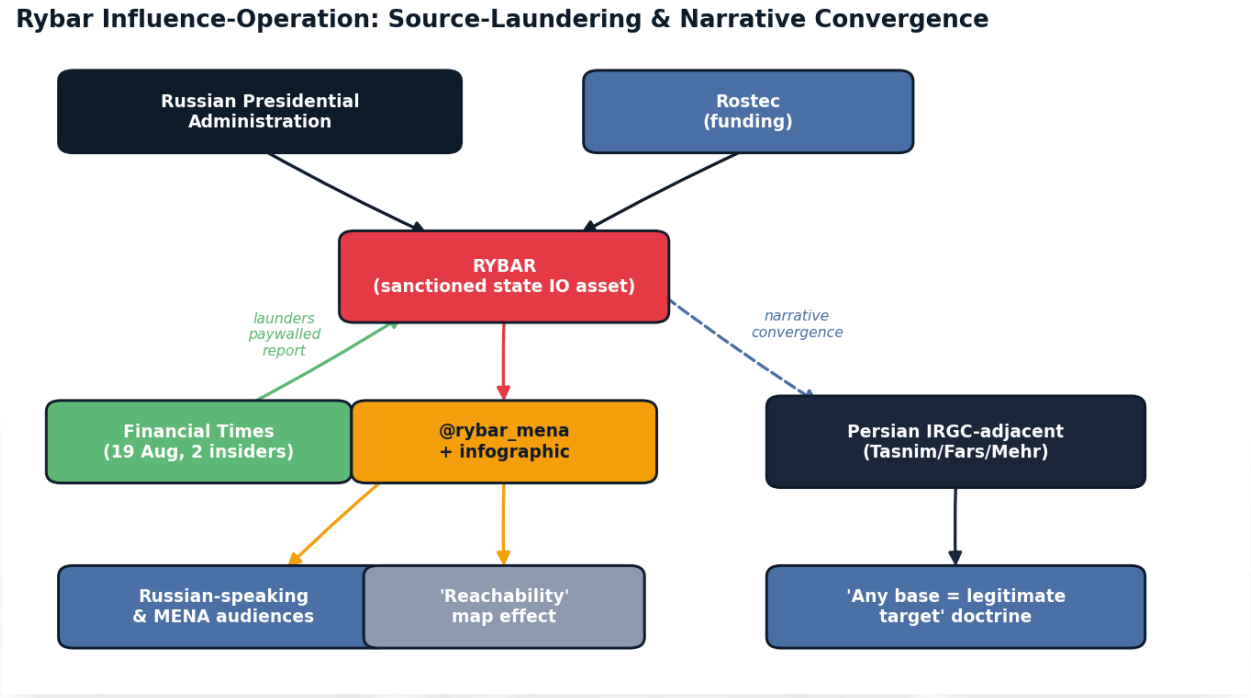
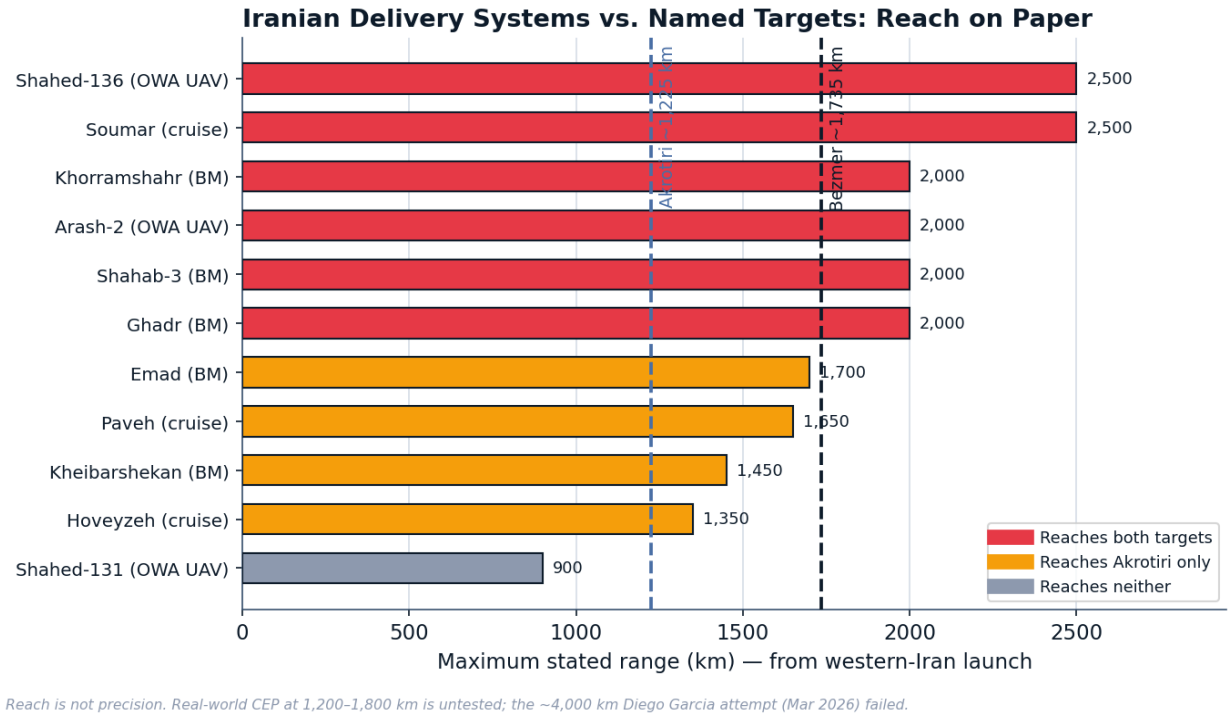


Figure 3. Source-laundering and narrative convergence. The Russian wedge frame ("US drags small allies into war") and the Persian doctrine frame ("any base is a legitimate target") converge and mutually amplify.

Deception assessment: No fabrication in the core facts. The primary technique is selective framing plus amplification/laundering of a Western-sourced story. Assessed intent (Likely, 55 to <85): advance Moscow's interest in prolonging US Middle East entanglement, raising European risk-aversion to hosting US forces, and normalizing critical-infrastructure attacks.

6. Capability Assessment: Reach, Precision, Magazine

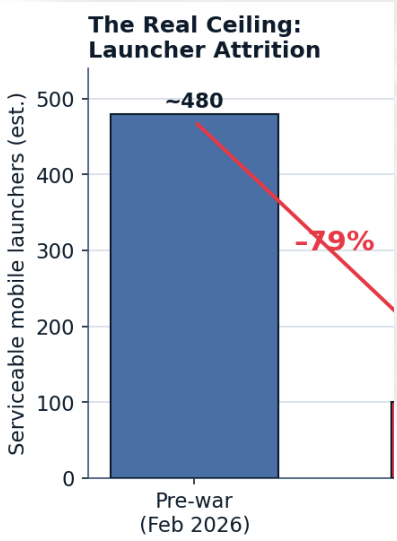
Distances first. The Tabriz area to Akrotiri is about 1,225 km, and to Bezmer about 1,735 km. From closer western-Iran launch points, both shrink. Rybar's infographic figures (~1,200 and ~1,800 km) are broadly accurate. **Reach is not in dispute. Precision effect is.**



Reach is not precision. Real-world CEP at 1,200–1,800 km is untested; the ~4,000 km Diego Garcia attempt (Mar 2026) failed.

Figure 4. Multiple ballistic, cruise, and one-way-attack systems range both targets on paper. The Shahed-136 (~2,500 km) and Arash-2 (~2,000 km) reach Bezmer directly, though slowly and via long, detectable overflight.

Accuracy in practice. Real-world CEP is poor. Middlebury analysts put the Emad's CEP near 1.2 km from the April 2024 strike on Nevatim. But it is improving in the 2026 war. The 17 July Jordan strike killed three US soldiers. Analysts link the gains to Russian satellite and SIGINT feeds, plus Chinese commercial imagery. At true European ranges (1,700+ km) against a defended base, that accuracy is untested. The ~4,000 km Diego Garcia attempt (20 March) failed.



Magazine and launchers. Pre-war, in February 2026, Iran held about 2,500 ballistic missiles and 480 launchers. After the ~40-day war: an estimated 500 to 1,000 long-range missiles, and only about 100 serviceable launchers. Rebuild runs at 100 to 300 missiles a month. June-2025 levels are possible by early-to-mid 2027. But the missiles are not the ceiling. The launchers are. That is why salvos taper after the first days.

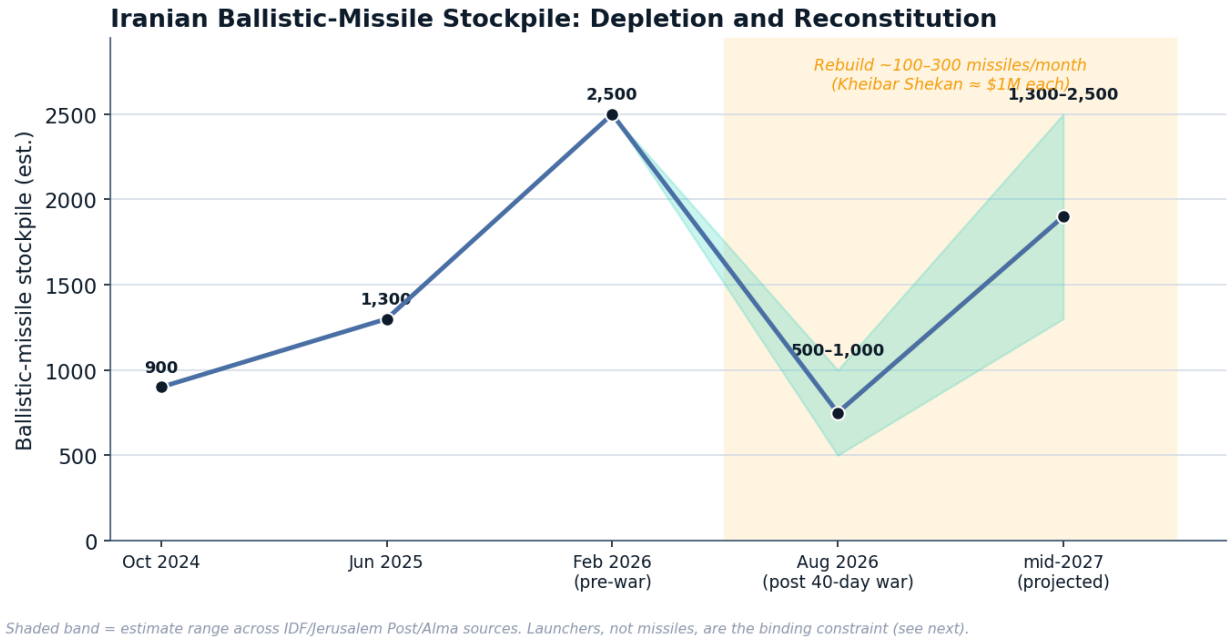


Figure 5. Depletion and reconstitution. Shaded band spans IDF / Jerusalem Post / Alma estimates.

7. Target-Selection Logic and Taxonomy

Iranian target selection is a signaling engine. It picks for deterrence, not damage. The record is consistent, from Abqaiq (2019) through Ain al-Asad (2020), True Promise I/II (2024), and Al Udeid (2025). Recurring criteria: symbolic fit to the triggering offense; a military function, never a civilian one; a target defended enough to call a "fortress" hit, with pre-warning to cap casualties; proportional signaling; deniability where Tehran wants no ownership; economic value where it exists. Europe fits the pattern. Bezmer and Akrotiri work as **threats**, precisely because striking them is escalatory.

7.1 Soft / Hard / Unsuspected taxonomy

Class / target	Purpose & intent	Feasibility	Confidence
HARD – Bezmer AB (Bulgaria)	Deterrence signaling; punish NATO host	Top of MRBM envelope; self-deterring	Threat persists: Likely (55 to <85)
HARD – RAF Akrotiri (Cyprus)	Signal E-Med reach; punish UK ISR (hangar hit Mar; reportedly U-2)	Demonstrated via proxy UAV	Repeat if war re-escalates: Roughly even (45 to <55)
SOFT – Shipping / Hormuz & Bab el-Mandeb	Economic coercion; price pressure	Demonstrated 2026	Highly likely (85 to <95) as lever
SOFT – Fuel/POL, warehouses, ports	Degrade US logistics with deniability	Proxy-dependent	Likely (55 to <85)
UNSUSPECTED – Undersea cables (Hormuz)	Economic 'digital chokepoint' pressure	Divers/UUVs; shallow strait	Threat Likely (55 to <85); cutting Roughly even (45 to <55)
UNSUSPECTED – Cyber / critical infra	Deniable coercion vs Europe	Documented capability	Likely (55 to <85), harassment

Class / target	Purpose & intent	Feasibility	Confidence
UNSUSPECTED – Diaspora / assassination	Transnational repression; retaliation-in-kind	Active, documented (Unit 840)	Highly likely (85 to <95) as most-used EU vector

Analytic judgment. The soft and unsuspected vectors fit best. They preserve deniability and sit below the Article 5 and Article 42.7 threshold. The hard NATO bases do neither.

Deterrence differs between Bezmer and Akrotiri. Bezmer is Bulgarian soil, undisputed NATO Article 5 and Article 6 territory. RAF Akrotiri is different. The Sovereign Base Areas of Akrotiri and Dhekelia are a British Overseas Territory under the 1960 Treaty of Establishment, and Cyprus is an EU member outside NATO. Article 6 of the North Atlantic Treaty fixes the geographic scope of Article 5, and whether the Sovereign Base Areas fall inside that box is contested and never tested.

The March 2026 strike settled the point in practice. When an Iranian-made drone struck Akrotiri, no NATO Article 4 or Article 5 consultation followed, and Cyprus raised Article 42(7) at the EU without invoking it. London ran a national response: the air-defense destroyer HMS Dragon and counter-drone Wildcats, on a bilateral commitment to Cyprus, not an Alliance one. The deterrence floor for Akrotiri sits below Bezmer's, and it has a demonstrated non-consultation precedent behind it. That asymmetry, not the range arc, is the target-selection driver. We assess it Likely (55 to <85) that any future Iranian or proxy action against the two bases again favors Akrotiri, the proven and legally softer target.

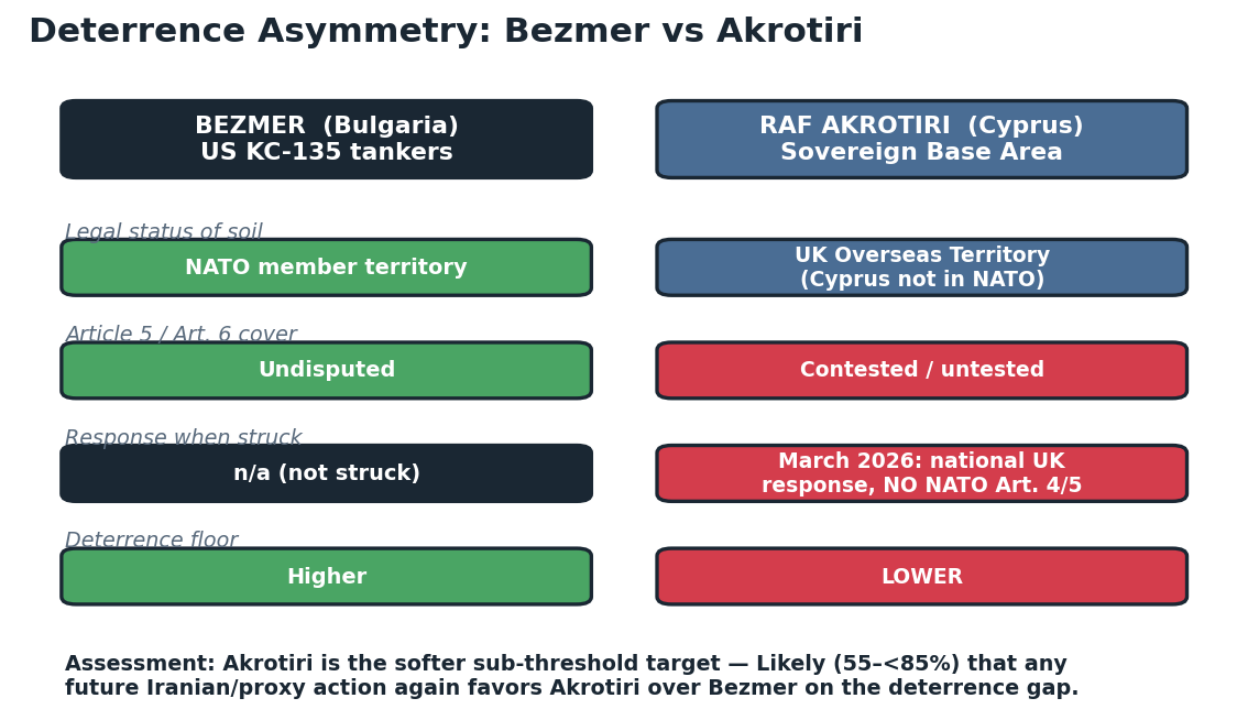


Figure 12. Deterrence asymmetry between the two named bases. Bezmer holds undisputed Article 5 cover; the Sovereign Base Areas do not, and the March 2026 strike drew a UK national response, not an Alliance one. Sources: North Atlantic Treaty Arts. 5–6; Treaty of Establishment 1960; Euronews, Fox, UK government statements (Mar 2026).

7.2 Wider candidate set (analyst-inferred, not FT-named)

The Financial Times named only three things: Bulgaria (Bezmer), Cyprus, and Hormuz subsea cables. It did not specify which Cyprus installations. The wider list is analyst extrapolation. Within claimed MRBM reach of the E-Med and Black Sea sit Souda Bay (Crete), Incirlik and other Turkey nodes, and Aegis Ashore Deveselu (Romania). Beyond comfortable

reach lie Aviano, Sigonella, and Vicenza (Italy). Gulf bases stay first-tier in any direct US–Iran round: Al Udeid, Al Dhafra, Ali Al Salem, Prince Sultan.

Displacement: the target may relocate, not disappear. One displacement question sits inside the wider set. If Sofia declines to extend past 1 October, the tankers do not vanish, they move. During the 2026 surge the KC-135 force already dispersed across Souda Bay on Crete, Rota and Morón in Spain, and Incirlik, and Romania authorized Mihail Kogălniceanu for US refuelling use in March 2026. The operationally logical receiving bases, Souda Bay and Mihail Kogălniceanu, sit inside claimed Iranian MRBM reach. Only a westward shift to Iberia moves the aircraft outside practical range, at a real operational-range cost. The threat mostly follows the tankers. We assess it Likely (55 to <85) that any relocation goes to Souda Bay or Mihail Kogălniceanu, keeping the aircraft inside the range rings.

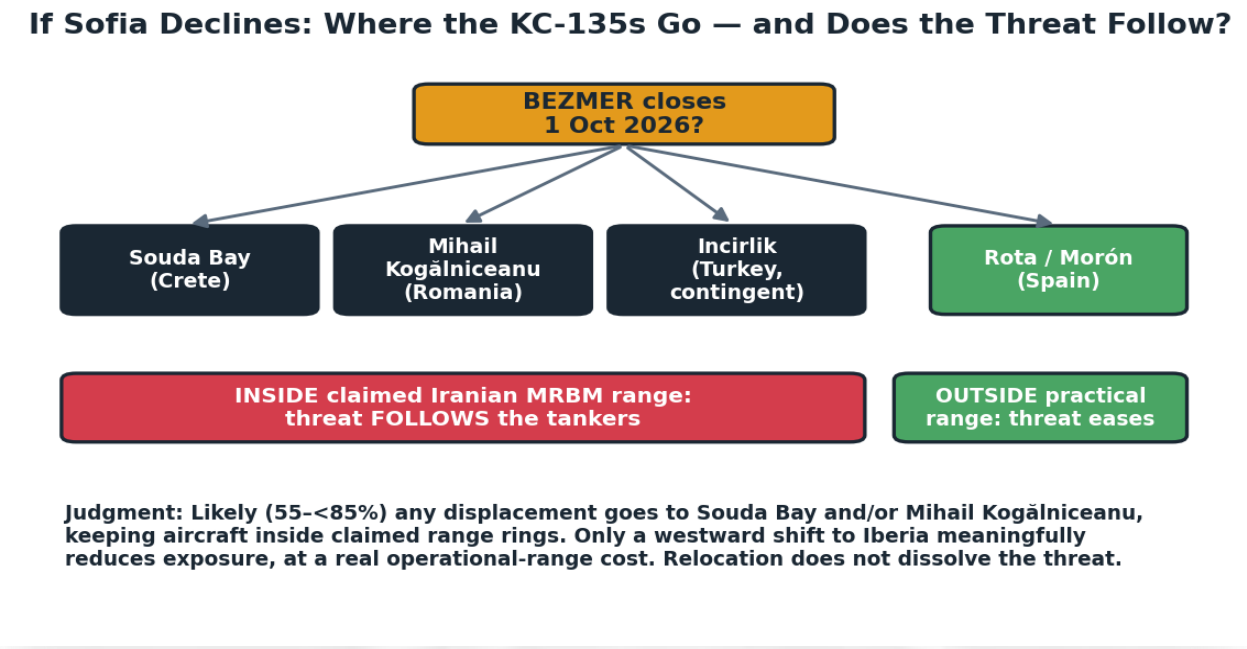


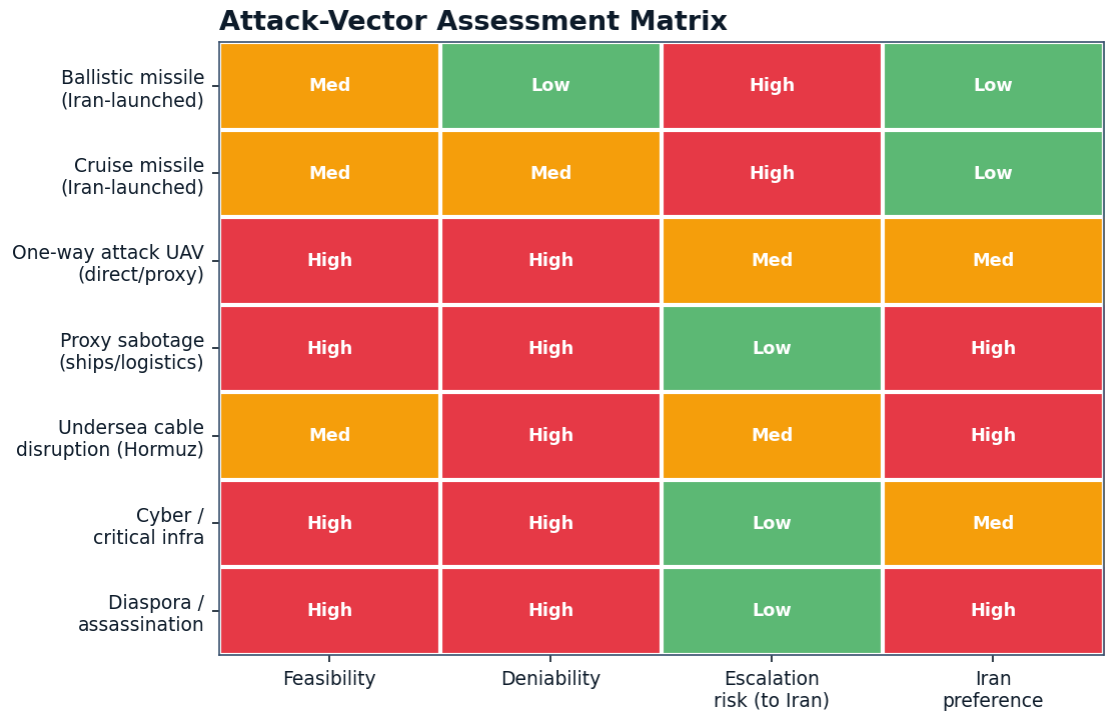
Figure 13. Tanker displacement if Bezmer closes. Most plausible receiving bases stay inside claimed Iranian MRBM range. Sources: Souda Bay OSINT tracking; Romania CSAT/parliament authorization (Mar 2026, via Bloomberg / Stars and Stripes); US–Greece MDCA.

7.3 Turkey: the pivot state nobody can route around

Turkey occupies four roles at once, and the report would be incomplete without naming them. It is a NATO ally hosting Incirlik and the Kürecik radar, both inside Iranian range and both covered by Tehran's declared doctrine that any base used against Iran is a legitimate target; roughly 1,500 to 1,700 US personnel are in country. Then there is the airspace problem: any Iranian ballistic or cruise shot toward Bulgaria crosses Turkish or Black Sea airspace, which raises detection, attribution, and third-party interception risk. Ankara also runs Iran's largest sanctions-evasion corridor, appearing in this report as a front-company node, a hawala hub, and a transit state for dual-use goods. Add to that a swing vote on allied cohesion. Iranian missiles were fired toward Turkey on 4 March 2026, and NATO air defenses engaged. Ankara's posture is a standing watch item rather than a settled input.

8. Attack Vectors and Feasibility

Score each vector on four axes: feasibility, deniability, escalation risk to Iran, and Iranian preference. The picture is clear. A mass ballistic salvo, the advertised vector, is the least likely. Deniable vectors are the most likely.



Green/Amber/Red = Low/Med/High. For 'escalation risk to Iran', High is a deterrent (bad for Iran). Diaspora & proxy-sabotage vectors score best for Tehran.

Figure 6. Attack-vector assessment matrix. For 'escalation risk to Iran', High functions as a deterrent. Diaspora and proxy-sabotage vectors score best for Tehran.

The demonstrated European vector is the one-way-attack UAV. On the night of 1 to 2 March 2026 a Shahed-type loitering munition hit Akrotiri. It was assessed Iranian-made, launched by a Lebanon-based proxy, and it struck a hangar, reportedly one holding US U-2 reconnaissance aircraft. From Lebanon, a proxy shot at Akrotiri (~250–350 km) is feasible, and it has already happened. Bezmer is the harder case. Direct Shahed-136 range suffices, yet the slow, hours-long, detectable overflight makes it a poor option.

9. Third-Party / Proxy Enablers (2026)

The 2024–2026 degradation reshaped the network. Assad's fall in December 2024 severed the Syrian land bridge. The center of gravity moved. It shifted from Hezbollah in the Levant to the Houthis in the Red Sea, and toward Iran's own missile, cyber, and clandestine tools for anything touching Europe.

Enabler	Vector enabled	2026 status (will + capability)
Houthis (Ansar Allah)	Red Sea / Bab el-Mandeb shipping	Most capable surviving arm; restarted attacks; threaten-use, not sea-control
Iraqi Shia militias (KH etc.)	Gulf & Iraq/Syria base harassment	Persistent capability; moderate willingness (self-preservation)
Lebanese Hezbollah	E-Med / Cyprus one-way-attack UAV	~80% rockets lost; drone 'leap' is short-range FPV; long-range Shahed class degraded but demonstrated 1 Mar
Russia	Targeting data, narrative, tech	Satellite + SIGINT + Kometa-M + Khayyam for the Middle East theater; NOT confirmed for a NATO-soil strike
China	Commercial satellite imagery	Sanctioned 8 May 2026 for imagery of US activity; 'eyes' half of the eyes-and-fist problem

Who runs Hezbollah now matters for the Cyprus vector. Naim Qassem has been Secretary-General since 29 October 2024, chosen after Israel killed Hassan Nasrallah on 27 September 2024 and his presumed heir Hashem Safieddine weeks later. Alma Research reads Qassem as a default pick, a founder and 30-year deputy who represents continuity of image rather than command talent, and who is working to recast the movement as a political actor inside Lebanon's system. He also faces a Lebanese cabinet disarmament plan and a UNIFIL mandate ending December 2026. Qassem warned in August 2025 that enforcing disarmament could bring civil strife. Hezbollah rejected the cabinet's phased plan on 17 February 2026, joined the war on 2 March, and in May Qassem called disarmament an existential threat. The organization's drone rebuild, run through Unit 127, has concentrated on short-range FPV systems for the border fight, not the long-range one-way-attack class needed to reach Cyprus. Taken together, a Qassem-led Hezbollah under disarmament pressure is a less willing deniable-launch partner than Nasrallah's was. That tempers the proxy-repeat estimate at the low end of Roughly even (45 to <55).

The diaspora vector is real and active. IRGC-Quds Force Unit 840 runs assassination and kidnap operations across Europe. It uses criminal proxies for deniability. The record is long: the London “Wedding” plot against Iran International anchors, the May 2025 arrest of five Iranian nationals over an Israeli-embassy plot in London, and a documented “German Network.” Fourteen governments condemned the campaign together in July 2025. Spring 2026 brought a wave of bombings and arson against Jewish and US-linked sites in Liège, Rotterdam, Amsterdam, Antwerp and London between 9 March and 29 April, claimed by Harakat Ashab al-Yamin al-Islamia, which the UK designated under its state-threats law in July 2026. This is Highly likely (85 to <95) to be Iran's most-used European vector.

10. Named Units, Suppliers, and Supply-Chain Interdiction

Capability rests on a chain of named organizations, foreign suppliers, and smuggling routes. That chain is physical and non-kinetic at once: hardware and propellant on one side; intelligence, espionage, and sabotage on the other. It has depth. Chokepoints run through it too. Map the nodes, and the disruption points appear.

10.1 Named Iranian units (order of battle)

Unit / organization	Role	Note
IRGC Aerospace Force (ASF)	Ballistic missiles and one-way-attack drones; the strike arm	Cmdr Hajizadeh killed June 2025; reconstituted
ASF Self-Sufficiency Jihad Org (SSJO)	Procures missile-applicable goods abroad	Oman/Turkey network sanctioned 2024
IRGC Navy (IRGCN)	Hormuz asymmetric fleet; mining, fast boats, shipping and cable harassment	Cmdr Tangsiri killed March 2026
QF Unit 190 (Transport)	Clandestine smuggling of arms, funds, and personnel worldwide	~20 members; B. Shahriyari (sanctioned)
QF Unit 700 (Logistics)	Military-equipment transfer to Hezbollah and Syria; maritime via Beirut	Humanitarian-aid cover
QF Unit 340	Rocket and missile R&D uplift for proxies (range, accuracy)	H. Fazeli (UK-sanctioned 2026)
QF Section 8000 / Unit 18000	Production and supply to proxies; Syria logistics and espionage	Syria land route degraded after Assad's fall
QF Unit 840	Assassination and kidnap in Europe via criminal proxies	UK-sanctioned 2024; EU sanctioned cmdr 2025
MOIS + IRGC Intelligence Org	Espionage, counterintelligence, surveillance	IRGC-IO director Khademi killed 2026
MODAFL / AIO / DIO	Defense-industrial production: missiles, propellant, TNT	

Unit / organization	Role	Note
Proxy receiving arms	Hezbollah Unit 4400 (receipt), Unit 127/200 (drones); Houthi missile and UAV arm	Forward-basing and re-export

10.2 Suppliers: what they provide, from where, by which route

Supplier	What it supplies	Origin → route → destination
China: MizarVision (Meentropy Technology, Hangzhou); The Earth Eye; Chang Guang Satellite Technology (Jilin-1 constellation)	Geospatial intelligence, AI-tagged US/allied base imagery, near-real-time carrier-tracking; earlier: sodium perchlorate, microelectronics, anti-ship-missile designs	Satellite feeds direct to IRGC-ASF targeting cell; component shipments Zhuhai / Guangzhou → IRISL vessels → Bandar Abbas / Chabahar. All three firms US-sanctioned 8 May 2026 (State Dept). Chang Guang had already supplied Houthis in 2025 and Wagner in Ukraine (sanctioned Dec 2023).
Russia (MoD / Rostec)	Drone components, TNT, ammunition; 'Russian-enhanced' Shahed tech; satellite imagery, SIGINT, Kometa-M anti-jam; Khayyam recon satellite	Caspian → 24+ ships → Amirabad / Bandar Anzali (NBC, Aug 2026)
DPRK (Munitions Industry Dept / KOMID)	Shahab-3 / Ghadr lineage (No-Dong derivative); Khorramshahr lineage (Musudan derivative); solid-fuel Sejjil design inputs via Shahid Haj Ali Movahed Research Center; specialty metals and igniters	Clandestine air and sea: DPRK engineers documented in Iran; technology barter (cash, oil, conventional arms). Shahid Hemmat Industrial Group (SHIG) designated partner (OFAC / UN). KOMID designated UN 2009; Fajr rocket line built under DPRK license.
Chinese logistics / chemical firms	Perchlorate supply and logistics (Shenzhen Amor Logistics; China Chlorate Tech; Yanling Chuanxing)	US-sanctioned Apr 2025; shipments continued
IRISL shipping	Maritime carriage of precursors and components	US-designated since 2008 (E.O. 13382); disables AIS tracking
Front-company procurement	Western microelectronics and dual-use goods	UAE, Turkey, Hong Kong, Malaysia → transship → Iran
Proxy nodes	Receive and forward ammonium perchlorate and arms; forward-basing	Houthis (Red Sea); Iraqi militias (land)

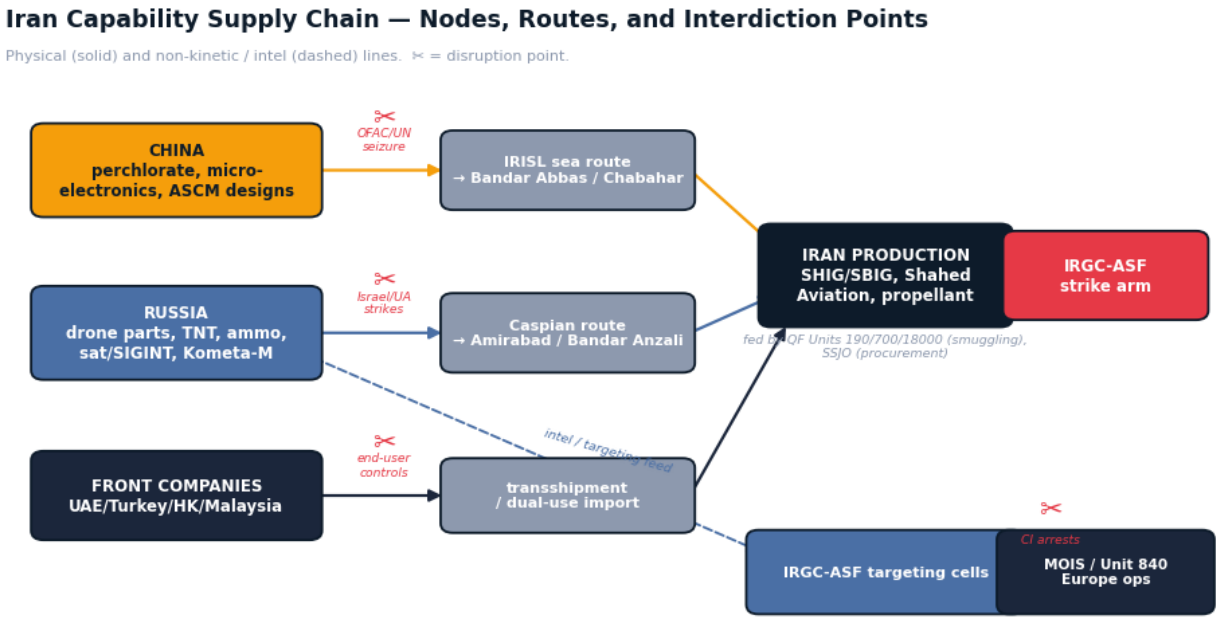


Figure 7. Iran's capability supply chain: physical lines (solid) and non-kinetic / intelligence lines (dashed), with interdiction points marked. Sources: NBC, WSJ, RFE/RL, FDD, gCaptain, Critical Threats, and US / UK / EU designations.

10.3 Non-kinetic supply chains: intelligence, cyber, espionage, sabotage, and finance

Intelligence targeting chain (collection → processing → strike). Iran's targeting pipeline for long-range strikes runs through four nodes. First, the Khayyam reconnaissance satellite, launched August 2022 on a Russian Soyuz from Baikonur, built on Roscosmos's Kanopus-V design, gives the IRGC an independently operated imaging platform over the Middle East for targeting and post-strike BDA. Second, Russian GRU feeds supplement Khayyam: satellite imagery and SIGINT on US naval and aircraft positions, reportedly including the Kometa-M anti-jamming system provided for CIA-linked Gulf targets (Al Jazeera, Jul 2026). Third, Chinese commercial providers: MizarVision used AI-enhanced algorithms to tag US aircraft, hardened shelters, and fuel storage; Chang Guang's 100+ Jilin-1 LEO satellites imaged carriers and P-8s in near-real-time; Earth Eye supplied imagery on request. Fourth, IRGC-ASF targeting cells at Dastvareh base integrate these feeds into strike packages. The July 2026 Jordan strike, which hit structures built after February 2026, indicates near-real-time construction monitoring. For a European strike, this chain faces a structural gap: Russian ground stations cannot collect over Europe without NATO detection, and China's LEO swarm cannot deliver the dwell-time needed for a contested attack on a defended NATO base. That gap is the primary reason European-range precision remains Unlikely to match Gulf-range precision.

Cyber supply chain. The IRGC and MOIS each run named APT clusters with documented European reach. APT33 (Peach Sandstorm / Elfin, IRGC) deploys Tickler and SHAPESHIFT wipers; it targets aerospace, satellite communications, energy, and defense contractors. OilRig / APT34 (Hazel Sandstorm, MOIS) uses DNS tunnelling and long-horizon spear-phishing, with documented infrastructure build-out impersonating UK tech companies in 2024–2025. Charming Kitten / APT35 / APT42 (IRGC-IO) runs credential-harvesting campaigns against journalists, policy researchers, and academics. Cotton Sandstorm / Emennet Pasargad (IRGC) has targeted Israel, France, and Sweden with cyber-enabled influence operations. CyberAv3ngers (IRGC-CEC) targets operational technology in water, energy, and transport. MuddyWater (MOIS) provides persistent access via PhonyC2 and commercial remote-management tools. UNC1860 and Smoke Sandstorm share infrastructure across MOIS and IRGC clusters. Tooling travels through bulletproof hosting in Russia and layered VPN exits; front domains frequently impersonate UK, German, and EU institutions. The US–Israel cyber offensive against Iran in late February 2026 drove Iran's internet to ~4% capacity and disrupted IRGC systems,

temporarily suppressing Iranian APT tempo. Augur Security (Aug 2026) assessed the lull as reflecting real disruption to operator safety, not a lasting capability loss.

Financial and hawala supply chain. Unit 840 pays European criminal proxies through a documented chain: IRGC handlers in Tehran contact Iranian criminal intermediaries (documented case: people-smuggler Ismail, recruited for the London 'Wedding' plot). Payment moves via hawala networks through the UAE, Turkey, and Malaysia. Cryptocurrency is an adjacent channel: IRGC-linked entities use Monero (privacy coin) and Tether on the Tron blockchain, per US Treasury designations. Shell companies in UAE free-trade zones and Malaysian holding companies provide layering. Documented amounts: the IRGC operative arrested in Europe admitted receiving $150,000 with $1 million promised on completion (Iran International, 2023). Iran's oil-sanctions-evasion network (IRISL-linked vessels, Caveh Shipping, and over 30 sanctioned entities, per OFAC Feb 2026) also funds general-purpose IRGC operations, including the European clandestine budget.

European espionage and sabotage supply chain. Three organizations run Iran's European human-intelligence and sabotage effort. Unit 840 (Quds Force): EU-sanctioned commander Mohammed Ansari (Jul 2025); field coordinator Yazdan Mir. The 'German Network' comprises three assassination squads targeting Iranian dissidents and Jewish citizens, documented by Iran International (Jan 2026). Named arrested operatives include Mansour Rasouli (admitted plots against an Israeli in Istanbul, a US general in Germany, and a French journalist) and five unnamed Iranian nationals arrested in London (May 2025). MOIS runs parallel European stations through embassy covers. After the 2018 Paris bomb-plot expulsion, MOIS shifted to criminal-proxy recruitment: the Lyon-based Turkish-origin trafficker 'Umit B.' (France), the Rumba criminal organization (Sweden), and drug-trafficking networks across the Netherlands and Denmark. Emennet Pasargad (Cotton Sandstorm) runs the Iran-state social-media manipulation arm; documented campaigns targeted French and Swedish audiences on the Iran war. Islamic cultural centers and charities in several EU capitals have been flagged by host-government services as MOIS or Quds Force-affiliated collection fronts; 14 governments jointly condemned the network in July 2025.

10.4 Interdiction and disruption assessment

Node / line	Vuln.	Disruption lever	Effect / precedent
China satellite imagery (MizarVision, Earth Eye, Chang Guang)	Medium	OFAC sanctions (8 May 2026); secondary pressure on customers; decoy infrastructure; GPS-spoofing	Partial: sanctioned firms continue; third-party re-selling not yet addressed. Decoys are the most scalable answer
Khayyam (Russia) satellite	Low	Cannot interdict a foreign satellite; deny access to ground truth via OPSEC, deception, camouflage	Degraded but not closed: OPSEC measures reduce what Khayyam captures
Russia GRU / Kometa-M anti-jam	Low–Medium	Demonstrate Kometa-M supply in legal forum; secondary sanctions on Rostec chain; EW countermeasures	US and EU evidence is public; full interdiction requires severing a state-to-state link
China perchlorate / components (sea)	Medium	OFAC / UN designations; port-state control; maritime seizure; end-user controls	Partial: IRISL AIS-spoofing and transshipment via UAE continue; seizures 2015–2025 demonstrate feasibility
Caspian route (Russia → Iran)	Medium	Sanctions; Israeli strikes on Bandar Anzali (Mar 2026); Ukraine struck vessels (Jul 2026); five transit-state pressure	Temporary rerouting recorded; no halt. Most vulnerable when vessels are in port
Houthi maritime supply	High	Arabian Sea interdiction; 19+ seizures 2015–2025; 750-ton NRF seizure Jul 2025; US blockade redirected 100 vessels by 23 May 2026 and 64 more after its July re-imposition	Best-demonstrated interdiction leg; not comprehensive (dhow volume exceeds boarding capacity)

Node / line	Vuln.	Disruption lever	Effect / precedent
IRGC-ASF production (SHIG / SBIG)	Medium (wartime)	US / Israeli kinetic strikes on 2,600+ military-industrial targets; destroyed ~80% of launcher pool	Launchers degraded 79%; missiles rebuilding 100–300/month; production harder to sustain-interdict than to degrade
Cyber infrastructure (APT34 / APT33 / MuddyWater)	Medium	Host-nation takedowns of C2; domain seizures; US / CISA / NCSC advisories; ISP-level blocking	Augur (Aug 2026): real disruption to operator safety post-war; lull assessed as temporary, not permanent loss
Financial / hawala (Unit 840 Europe)	High	Track, freeze, and seize hawala networks; OFAC crypto designations (Tether/Tron chain); correspondent-bank pressure on UAE and Turkey	Highest feasibility: payments are the chokepoint for criminal-proxy recruitment
Unit 840 European espionage	High	Counterintelligence arrests; embassy expulsions; disrupt criminal-proxy cut-outs	Demonstrated: London arrests May 2025; Paris expulsion 2018; 14-govt condemnation Jul 2025
MOIS front organizations in Europe	Medium	Proscription; asset freezes; charity-commission investigations	Slow but persistent: several EU states have already listed specific centers

Where interdiction bites. The physical chain has three real chokepoints: the sea lane from China, the Caspian ships from Russia, and the front-company nodes in the Gulf and Asia. None can be closed outright, and the record shows why. Sanctions in April 2025 did not stop the perchlorate, and strikes on Bandar Anzali only rerouted the Caspian traffic. The better return is cumulative pressure. Sanctions, seizures, and counterintelligence together raise cost and slow tempo, where a single cut cannot. The non-kinetic lines are the softer target. Counterintelligence has already broken Unit 840 cells in Europe, and sanctioning the satellite providers is a cleaner move than chasing every chemical cargo.

11. Economic Coercion: The Sharper Lever

Rybar's own read holds up. Economic damage bites hardest in the medium term, and the data agree. About 20 million barrels a day of oil, roughly a fifth of global petroleum liquids consumption, transits Hormuz (EIA). The IRGC declared closure on 2 March 2026. Brent's April peak touched $126 intraday, with physical cargoes reported near $150. War-risk premiums jumped from about 0.2% to 1% of hull value per transit within 48 hours. Traffic fell to roughly 10 vessels a day, against an 88 to 130 baseline. The Dallas Fed models a global GDP hit of up to 1.3 points if closure runs three quarters.

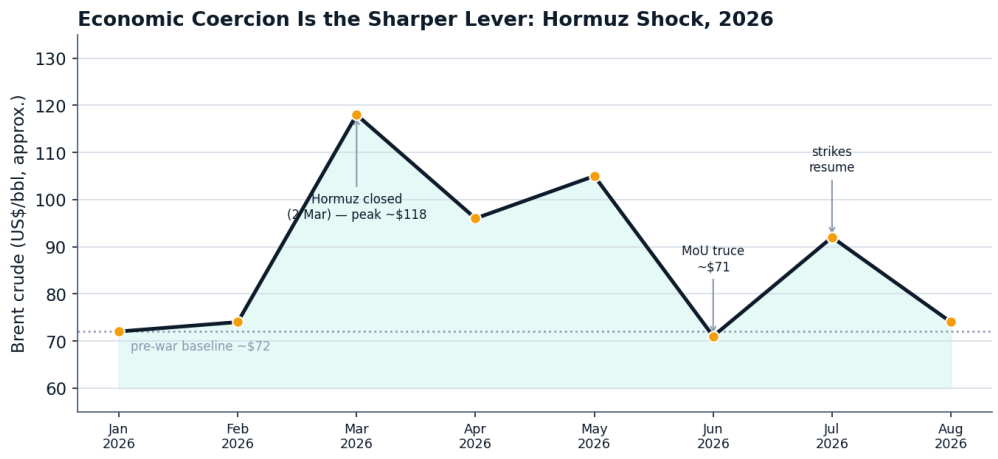


Figure 8. The Hormuz shock, 2026. Prices eased toward pre-war levels during the truce, then re-escalated. Sources: Dallas Fed, Brookings, World Bank, Howden Re, IMF PortWatch, CRS, CNBC.

12. Outlook: Scenarios and Cones of Plausibility

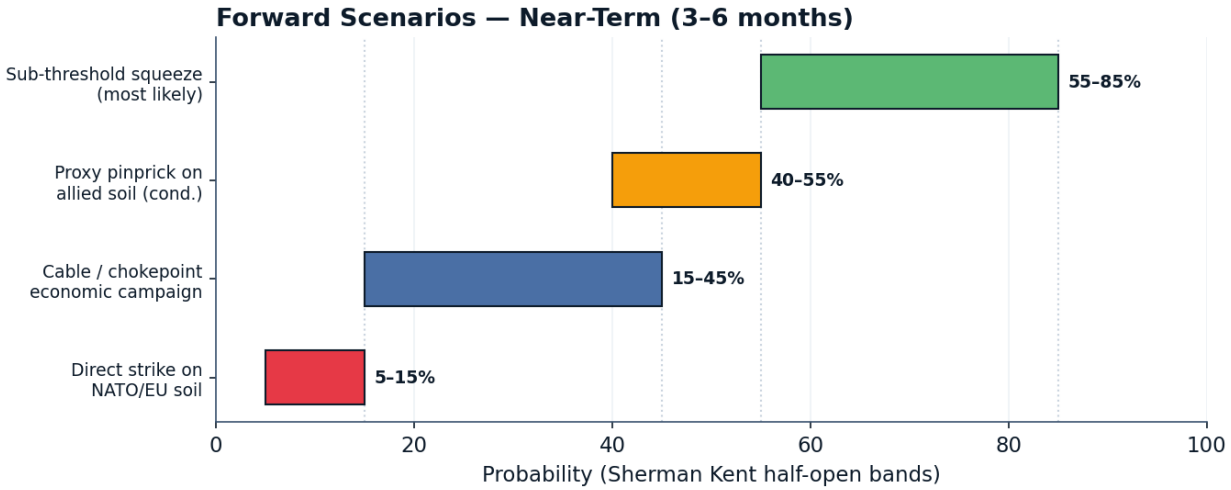


Figure 9. Near-term (3–6 month) scenarios with Sherman Kent bands.

- **Sub-threshold squeeze (Likely, 55 to <85).** Contingency planning and signaling continue; kinetic action stays in the Gulf/Red Sea and, at most, proxy UAV harassment of E-Med assets. No direct strike on Bezmer/Akrotiri.
- **Proxy pinprick on allied soil (Roughly even, conditional).** A repeat Akrotiri-style deniable strike after a US or Israeli escalation.
- **Chokepoint and cable campaign (Unlikely, 15 to <45). Cable cutting and closure operations beyond the current shipping squeeze, medium-term economic pain, no NATO-soil crossing.**
- **Direct strike on NATO/EU soil (Unlikely, low end of 15 to <45).** Requires a major new US strike inside Iran as the trigger; the option Rybar itself argues would backfire.

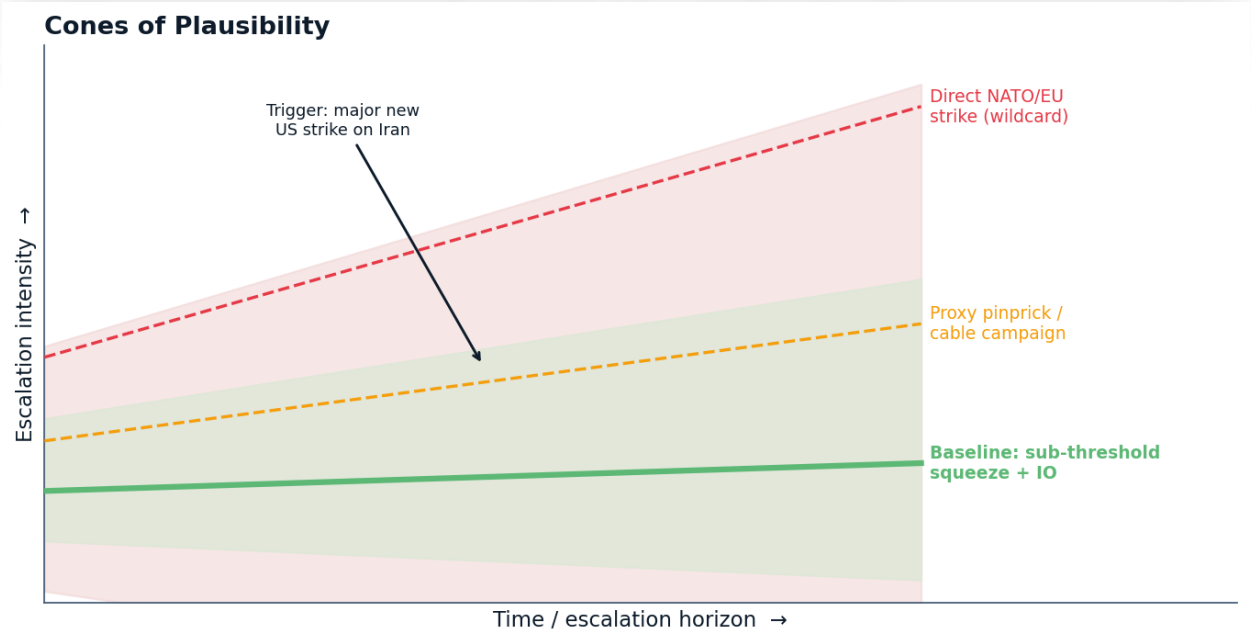


Figure 10. Cones of plausibility. The baseline holds unless a major US escalation pushes the trajectory into the wildcard cone.

13. Structured Analytic Techniques

13.1 Analysis of Competing Hypotheses

Hypothesis	Assessment
H1 – Genuine intent to strike Europe	Weakly supported; no diagnostic pre-positioning observed
H2 – Contingency planning + coercive signaling	Best supported; fits FT wording and Iranian doctrine
H3 – Russian IO amplifying a real story	Strongly supported as the framing layer; not mutually exclusive with H2
H4 – Fabrication	Rejected; core facts independently verified

ACH conclusion: H2 substance carried on an H3 vehicle. Real contingency planning and signaling, opportunistically amplified by a directed Kremlin asset.

13.2 Key Assumptions Check

- Article 5 / 42.7 deters a direct strike: holds, with caution given a hardliner regime that could miscalculate.
- Iranian long-range accuracy is poor: holds on 2024/Diego Garcia evidence, but improving with Russian/Chinese support; treat as a watch-item.
- The Akrotiri drone was proxy-launched from Lebanon: holds, single-nation attribution (Cypriot FM).
- Western powers still hold a UN-sanctions lever: fails. E3 snapback completed on 27 September 2025, before this war. All six prior UN sanctions resolutions are back in force, and enforcement is fractured across the P5 after Russia and China contested the trigger. No October 2026 Resolution 2231 date coincides with the Bezmer window. The card is spent, which lifts Iran's freedom of action on the UN track at the margin.

13.3 Indicators & Warning

Indicator	Direction	Value
Resumed major US strikes on Iranian infrastructure	Escalatory	High
MRBM/TEL movement toward NW/W Iran	Escalatory	High
Forward-staging of proxy UAVs toward the E-Med	Escalatory	High
Cable-repair vessel harassment in Hormuz	Escalatory (econ.)	Medium
Rybar/Persian 'legitimate target' messaging surge	Narrative	Medium–High
Diplomatic re-engagement / Hormuz normalization	De-escalatory	High
Bulgarian extension-vote signals / Sofia coalition motion on Bezmer	Political	High

14. Evidence Layer: ASA Tri-Score and Admiralty

ASA Tri-Score (artifact set). T: Mature D: High (~60, floor 25) F: Operational

Evidence quality is Mature. The factual substrate is strong and multi-sourced. Deception likelihood is High: a decapitated hardliner regime with a calculated-ambiguity habit, amplified by a directed IO asset. Forecast confidence is Operational. The near-term behavioral forecast is well-grounded, but the widened intent band and untested European-range precision cap it. **Cross-score posture:** confident on the pattern, alert to deception, cautious on timing.

14.1 Triple endgame

- **Stated:** “no limits”; hit Europe if the US strikes Iranian infrastructure; sovereign control over Hormuz.
- **Optimal (from realized position):** maximize coercion and split allied resolve without triggering Article 5 / 42.7; win the perception war, keep the off-ramp.
- **Most-Likely Achieved:** a prolonged “neither war nor peace” holding pattern with deniable action and information operations; Bezmer/Akrotiri stay rhetorical hostages.

14.2 Admiralty (NATO 6×6) on key sources

Source / claim	Grade	Note
FT (19 Aug) – Europe targeting	B2–B3	Two anonymous regime insiders
Bezmer KC-135 vote (22 Jul)	A1	Official parliamentary record
Akrotiri drone → Lebanon (Mar)	B2	Official but single-nation attribution
Russian/Chinese targeting support	B2	Consistent multi-source; partial official confirmation & caveat
Missile rebuild rate (Aug)	B2–C3	Israeli-sourced; consistent with prior recovery
Rybar / @rybar_mena	E	Directed state IO asset; artifact value only

15. Intelligence Gaps and Collection Requirements

Two gaps most change the answer and cannot be closed from open source; they should drive tasking.

PIR	Requirement	Why decisive
PIR-1	Does Iran hold actual target packages for Bezmer/Akrotiri, or only an assessment?	Separates gesture from capability
PIR-2	Would Russia provide targeting-grade support for a NATO/EU-soil strike?	The hinge from 'gesture at Europe' to 'hit Europe'
PIR-3	True Iranian MRBM CEP at 1,200–1,800 km vs a defended base	European-range precision is inferred, not observed
PIR-4	Residual Hezbollah long-range (non-FPV) OWA-UAV inventory	Underpins any Cyprus repeat
PIR-5	Mojtaba Khamenei's risk tolerance on horizontal escalation	Untested on the NATO question
PIR-6	Bezmer nearer-launch pathway (maritime / Black Sea / covert)	Currently no evidence
PIR-7	Iranian intent and capability vs Mediterranean cables (beyond Hormuz)	The aspirational leap toward Europe
PIR-8	Rybar / Persian-language amplification of the Bezmer–Akrotiri frame, and Mojtaba-era regime cohesion under economic collapse	Ties the influence-operation tempo and the diversionary-escalation tail to observable indicators

16. Recommendations

Recommendations are ranked by risk priority, then sequenced by when execution must begin. Risk rating combines likelihood (Sherman Kent band) with impact (1–5). Two lines carry the most risk: the influence operation, which is running now, and the diaspora vector, which is Iran's most-used tool in Europe. Both start today, and the rest follow in order.

#	Action	Risk it addresses	Rating	Start	Owner
R1	Counter the IO: pre-bunk and attribute the Rybar 'hostage-target' frame with host-nation publics	Allied cohesion erosion; host-nation resolve	CRITICAL	Now	StratCom / IO cell
R2	Activate diaspora-threat protection and criminal-proxy monitoring	Assassination / kidnap (Unit 840)	CRITICAL	Now	Host security services
R3	Harden Akrotiri and Bezmer against one-way-attack UAS; layer counter-drone	Proven proxy-UAV vector	HIGH	0–30 d	Force protection
R4	Protect shipping, logistics, and Hormuz cable-repair; build routing and cable redundancy	Economic coercion	HIGH	Now	Maritime domain / insurers
R5	Stand up the PIR-1 / PIR-2 I&W watchboard and collection	Strategic surprise	HIGH	0–30 d	Intel / collection
R6	Pre-plan NATO Article 5 and EU Article 42.7 consultation tracks	Low-probability, high-impact strike	MEDIUM	30–90 d	Policy / legal
R7	Preserve a visible off-ramp for Tehran in messaging and posture	Miscalculation / spiral	MEDIUM	Continuous	Policy

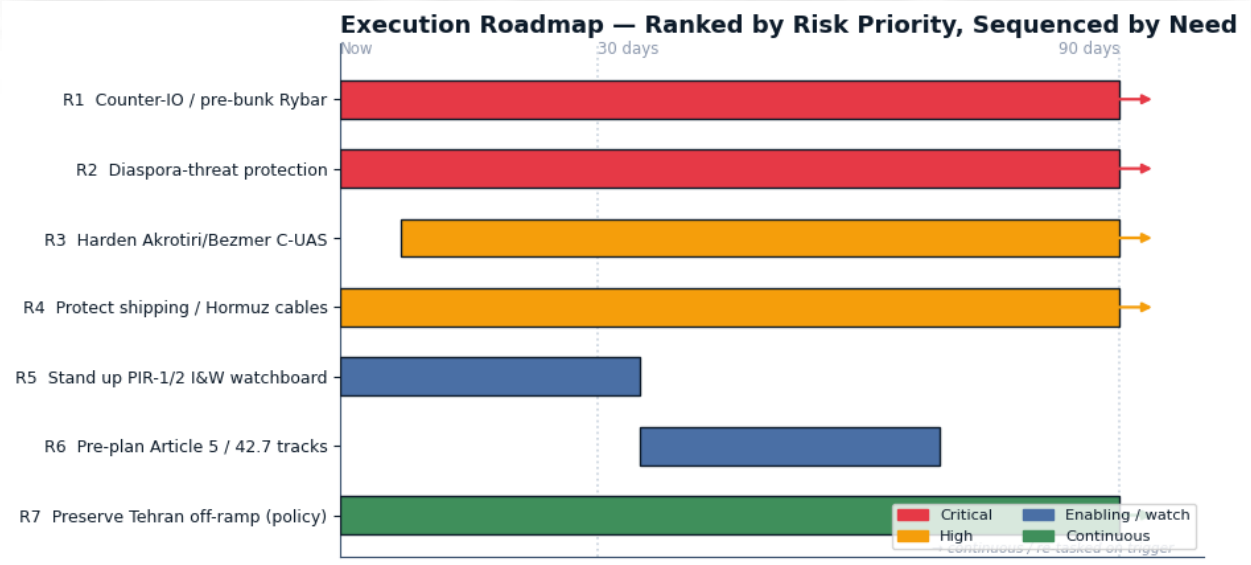


Figure 11. Execution roadmap. Bars ranked by risk priority and sequenced by start-need; arrows denote continuous or trigger-retasked effort.

Residual risk after action: Moderate and mostly transferred to the deniable and economic vectors, which no single measure removes. The direct-strike tail stays Unlikely and is best held there by preserving Tehran's off-ramp (R7). Revisit on any I&W trip, and at 90 days regardless.

17. Caveats and Sourcing

Facts and adversary/source claims are kept separate throughout. The FT-reported European options are assessed contingencies, not an ordered strike. Iranian "legitimate target" and cable-"fees" statements are propaganda, not enacted policy. Rybar is non-neutral by design; factual overlaps reflect that it copied verifiable reporting.

Single-thread items: the FT (two anonymous sources), the Cypriot attribution of the Akrotiri drone, and some Wikipedia 2026-war casualty/attribution figures each carry attribution risk and were cross-checked where possible. Capability figures (stockpile, launchers, CEP) span a source range and are presented as bands.

Overall confidence: Moderate-to-High on the pattern and the sub-threshold-preference judgment; Moderate on scenario probabilities; Low-to-Moderate on timing and on Iranian long-range precision against defended European targets.

No operational content is included by design. This is a strategic, analytic, defensive product using only public open-source reporting. Probability language uses Sherman Kent half-open bands.

Sources consulted (Aug 2026): Financial Times via Iran International / Kyiv Post / Israel Hayom / i24 / Ynetnews / EUalive; Al Jazeera; Washington Post; NPR; CNN; CBS News; Jerusalem Post; Times of Israel; SIPRI; FDD & FDD Long War Journal; Alma Research and Education Center; Foreign Policy; Foreign Affairs; AEI Critical Threats; Washington Institute; ICCT; Greydynamics; Dallas Fed; Brookings; World Bank; Howden Re; CRS/Congress.gov; CNBC; Novinite; BTA; Army Recognition; Forces News; CSIS Missile Threat; Britannica; GOV.UK; Wikipedia 2026-war article set. Adversary/state-linked outlets (Rybar, Tasnim, Fars, TASS) characterized analytically, not relied upon as fact.