ECONOMIC | Financial Warfare, Sanction-Busting Ecosystems, and Market Volatility

submitted by sar_jay

EXECUTIVE SUMMARY

Iran's shadow fleet and its associated financial architecture have evolved from a sanctions-evasion mechanism into the primary engine sustaining the Islamic Republic through active armed conflict. Since the United States and Israel launched Operation Epic Fury on 28 February 2026, the Strait of Hormuz has been effectively closed, with vessel transits collapsing from approximately 130 per day in February to a near-complete halt by March. The economic consequences now constitute the largest disruption to global oil markets in recorded history, according to the International Energy Agency. The conflict has simultaneously exposed three converging vulnerabilities: Iran's dependence on a sophisticated black market infrastructure to fund its war effort; the world economy's structural reliance on a 21-mile navigable corridor; and the "Economic Kill Switch" embedded in GCC desalination infrastructure, whose destruction threatens to convert energy war into humanitarian catastrophe. This report audits the loss event frequency, quantifies financial impact across targeted nations, maps adversary infrastructure, and delivers actionable intelligence for CFOs, maritime underwriters, and trade compliance teams.

SECTION 1: ADVERSARY INFRASTRUCTURE — THE SHADOW FLEET IDENTITY FRAUD ARCHITECTURE

1.1 Scale and Current Operational Status

In 2025 alone, OFAC sanctioned more than 875 persons, vessels, and aircraft as part of the US maximum pressure campaign. Since NSPM-2 was issued in February 2025, the total has exceeded 1,000 designations. Despite this, Iran's shadow fleet continues to operate. As of April 2026, Windward AI has documented Iran moving tens of millions of barrels through covert offshore

transfer networks to bypass the US blockade, using ship-to-ship transfers conducted beyond the blockade perimeter. On 20 April 2026, US Central Command confirmed that US Marines boarded and seized the Iranian-flagged M/V Touska after it attempted to violate the naval blockade — the latest in a series of active interdiction events. Lloyd's List reported the same day that shadow fleet vessels are continuing to operate even under heightened military pressure.

[TankerTrackers AIS playback, 17 April 2026: Sanctioned tankers entering and departing the blockade zone with ease along the eastern Oman-Pakistan line]

[WSJ-cited breaking report: Over 25 Iranian-linked oil and gas tankers successfully evaded US blockade in the Strait of Hormuz]

These two open-source signals — one from a maritime intelligence firm's AIS playback, one from a breaking WSJ-sourced report — confirm that the blockade is experiencing active, systematic penetration by sanctioned vessels, not isolated incidents.

The October 9, 2025 OFAC action — the broadest single Iran energy-sector designation of that year — sanctioned over 50 individuals, entities, and vessels collectively enabling the export of billions of dollars' worth of petroleum and liquefied petroleum gas (LPG). The action targeted a network moving hundreds of millions of dollars' worth of Iranian LPG, nearly two dozen shadow fleet vessels, the China-based Rizhao Shihua Crude Oil Terminal, and the independent Shandong Jincheng Petrochemical teapot refinery. UAE-based Markan White Trading Crude Oil Abroad Co. L.L.C and Slogal Energy DMCC were identified as key enablers, with Markan White facilitating tens of millions of dollars' worth of LPG sales on behalf of Iran's Persian Gulf Petrochemical Industry Commercial Co (PGPICC), and using Hong Kong-based shell companies Ravenala Trading Co. and Crimson Blue Trading Co. to process over

$100 million in payments. Slogal purchased Iranian LPG delivered to Sri Lanka and Bangladesh across 2024 and 2025.
Despite these escalating designations, Windward AI data confirms that of approximately 430 tankers currently engaged in Iranian trade as of early 2026, roughly 62 percent are falsely flagged and 87 percent are already sanctioned. The Marshall Islands, Hong Kong, China, and Panama represent the top four jurisdictions of incorporation for registered owners of this fleet, reflecting how ownership structures are deliberately distributed across global maritime registries to complicate enforcement.
The structural dynamic confirmed by TankerTrackers is one of diminishing marginal enforcement impact: the designation rate has never matched the available pool of vessels willing to join the shadow ecosystem. Iran Iran has used this excess supply to offer crude at steep discounts — Germany-based BPT Berlin Petroleum Trading GmbH was documented seeking to purchase millions of barrels of Iranian crude in early 2025, with Iran offering a $17 per barrel discount to attract buyers despite sanctions risks.

1.2 The Three Core Evasion Mechanisms

AIS Identity Fraud and Signal Manipulation. Vessels employ three distinct AIS deception methods. The first, "going dark," involves complete transponder shutdown. The second, spoofing, involves broadcasting false location and identity data that appears normal on tracking systems while the vessel moves elsewhere. The third involves impersonating legitimate vessels by feeding their IMO numbers into falsified documentation. A vessel documented by The Jerusalem Post spoofed its position for eleven days while carrying approximately 250,000 barrels of methanol, officially logged as loaded at a UAE port but originating from Iran.

The WikiIran vessel identity theft programme, uncovered through leaked server data from Shahid Abolfathi Oil Command, is the most operationally significant finding in this investigation. Sepehr Energy Jahan (SEJ), designated by OFAC and identified as the Iranian Armed Forces General Staff (AFGS) oil export front company, is not merely renaming sanctioned vessels. It is stealing the documented identities of legitimate, non-sanctioned vessels operating under clean flags.

VESSEL REAL NAME:	LIMAS						TC COST:			$3,672,000.0
VESSEL FAKE NAME:	KALLISTA						FUEL PURCHASE:			$785,344.0
TC RATE PER DAY:	$54,000.00						FUEL ONBOARD:			$2,447,786.4
TITLE	QUANTITY AS PER NOON REPORT		VSL CONSUMTION AS		FUEL PURCHASE		VSL CONSUMTION AS PER NOON REPORT CHECK BY		COVERED DISTANC	DIST STEAMED PER DAY
	VSFO	MGO	N/A				N/A			
FUEL ON DELIVERY	1,420.50	196.00	VSFO	MGO	VSFO	MGO	VSFO	MGO	N/A	
19-Dec-24							0.00	0.00	332.00	332.00
20-Dec-24							0.00	0.00	1,859.00	1,527.00
21-Dec-24							0.00	0.00		-1,859.00
22-Dec-24							0.00	0.00		0.00
23-Dec-24							0.00	0.00		0.00
24-Dec-24							0.00	0.00		0.00
25-Dec-24	4,666.70	780.80	64.00	2.20			-4,666.70	-780.80		0.00
26-Dec-24	4,599.80	778.40	66.90	2.40			66.90	2.40		0.00
27-Dec-24	4,535.80	776.10	64.00	2.30			64.00	2.30	323.00	323.00
28-Dec-24	4,472.00	773.80	63.80	2.30			63.80	2.30	333.00	10.00
29-Dec-24	4,408.30	771.50	63.70	2.30			63.70	2.30		-333.00
30-Dec-24	4,343.10	769.10	65.20	2.40			65.20	2.40	345.00	345.00
31-Dec-24	4,280.20	766.80	62.90	2.30			62.90	2.30	354.00	9.00
1-Jan-25	4,215.20	764.50	65.00	2.30			65.00	2.30		332.00

VESSEL REAL NAME:	LIMAS
VESSEL FAKE NAME:	KALLISTA

IN THE NAME OF THE ALMIGHTY

NATIONAL IRANIAN OIL COMPANY

BILL OF LADING

Shipped in apparent good order and condition by **NATIONAL IRANIAN OIL COMPANY**
on board the **PANAMANIAN** motorship **KALLISTA**
Whereof **ZHOU SUOSHENG** is Master at the port of **KHARG ISLAND, IRAN.**
a quantity said to be **1,044,598** **US.BARRELS** of **PARS CRUDE OIL**
equal to : **145,330.203** long tons **147,662.303** metric tons . **27.30** API at 60F , the quantity , measurement , weight , gauge , nature , value and condition of the cargo unknown to the vessel and the Master , to be delivered at the port of **DALIAN PORT, CHINA.**

or so near thereto as the Vessel can safely , get always afloat , unto
ORDER OF SEPEHR ENERGY JAHAN NAMAYE TABAN CO.

COPY NOT NEGOTIABLE

"TRANS SHIPMENT NOT ALLOWED"
or order on payment of freight at the rate of
"INSURANCE AND FREIGHT PAYABLE AS AGREED."
This shipment is carried under and pursuant to the terms of the charter dated
at between
and as charterer , and all the terms whatsoever of the said charter except the rate and payment of freight specified therein apply to and govern the rights of the parties concerned in this shipment .

If this Bill of Lading is a document of title to which the Carriage of Goods by Sea Act of the United States , Approved April 16 , 1936 , or similar legislation giving statutory effect to the International Convention for the Unification of certain rules relating to Bills of Lading at Brussels of August 25 , 1924 , applies by reason of the port of loading or discharge being in territory in which the said Act or other similar legislation is in force , this Bill of Lading shall have effect subject to the provisions of the said Act or other similar legislation , as the case may be , which shall be deemed incorporated herein , and nothing herein contained shall be deemed a surrender by the carrier of any of its rights or immunities or an increase of any of its responsibilities or liabilities under said Act or other similar legislation . If any term of this Bill of Lading is repugnant to the said Act or other similar legislation as so incorporated , such terms shall be void to that extent but no further .

In witness whereof , the Master has signed **(3)** Bill of Lading of this tenor and date , one of which being accomplished , the others will be void .

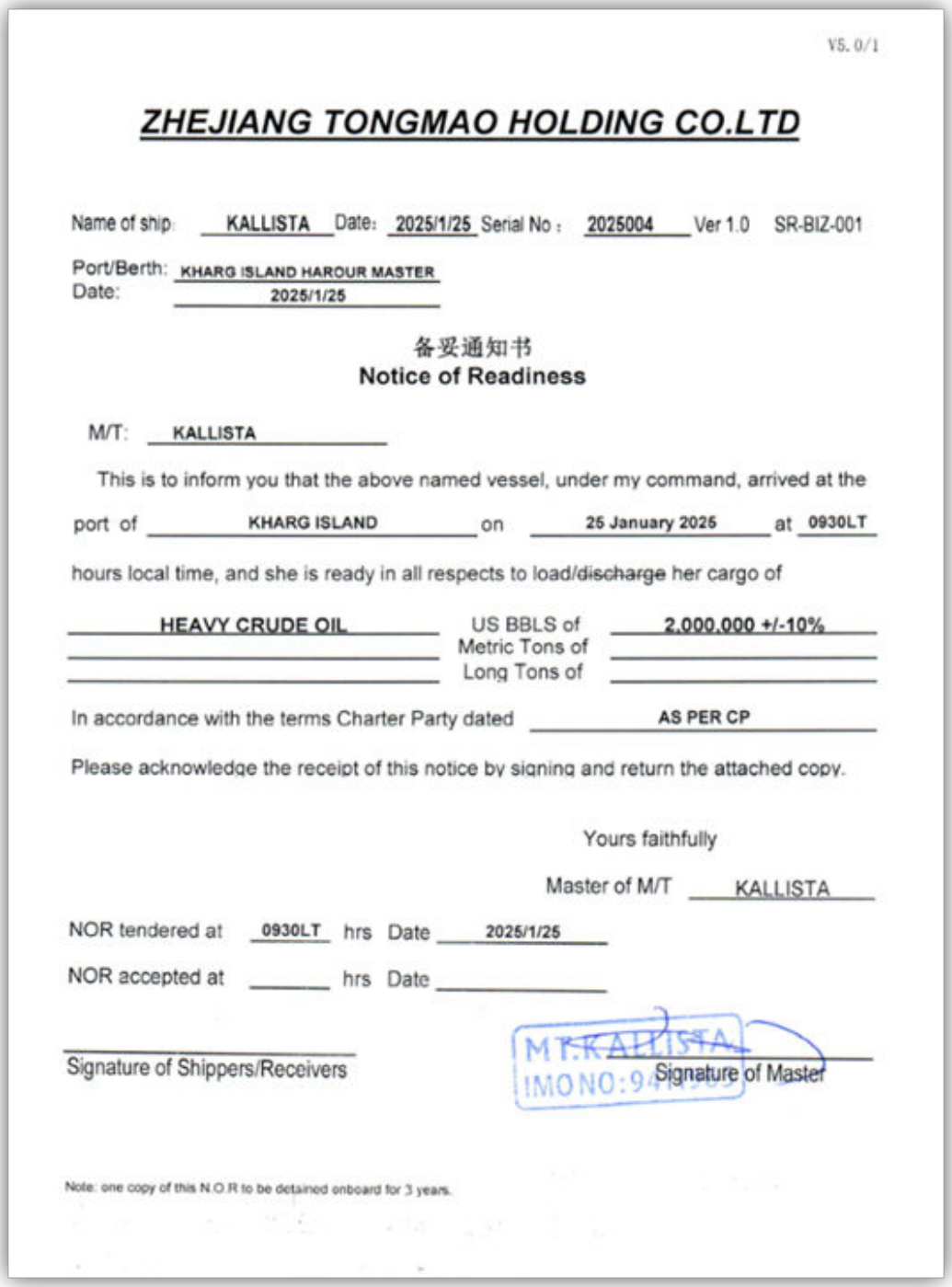
Dated at **KHARG ISLAND, IRAN.** this **Thursday, 19 December, 2024**

WARSHIPOILVOY BILL OF LADING .

MT.KALLISTA
IMO NO : 9411[illegible]

SER.NO **0510/24**

MASTER ZHOU SUOSHENG



V5.0/1

ZHEJIANG TONGMAO HOLDING CO.LTD

Name of ship: KALLISTA Date: 2025/1/25 Serial No: 2025004 Ver 1.0 SR-BIZ-001

Port/Berth: KHARG ISLAND HAROUR MASTER
Date: 2025/1/25

备妥通知书
Notice of Readiness

M/T: KALLISTA

This is to inform you that the above named vessel, under my command, arrived at the port of KHARG ISLAND on 25 January 2025 at 0930LT hours local time, and she is ready in all respects to load/~~discharge~~ her cargo of

HEAVY CRUDE OIL — US BBLS of 2,000,000 +/-10%
Metric Tons of
Long Tons of

In accordance with the terms Charter Party dated AS PER CP

Please acknowledge the receipt of this notice by signing and return the attached copy.

Yours faithfully

Master of M/T KALLISTA

NOR tendered at 0930LT hrs Date 2025/1/25

NOR accepted at _____ hrs Date _____

Signature of Shippers/Receivers

M.T.KALLISTA
IMO NO:9411965

Signature of Master

Note: one copy of this N.O.R to be detained onboard for 3 years.

The leaked data includes records of over 100 vessels facilitating illegal crude export. Among them, 20 are already OFAC-sanctioned yet continue operating. The clearest documented case involves KALLISTA (IMO 9411965), whose internal SEJ documentation labels it a "Vessel Fake Name," with LIMAS (formerly KOHANA, IMO 9254082) as the real vessel. Expenses tied to voyages made under the stolen identity align temporally with Iranian crude shipments.

VESSEL REAL NAME:	SARAK
VESSEL FAKE NAME:	FLEVES

In a separate documented case, SEJ agents obtained original certification documents from the FLEVES (IMO 9597006), a legitimate Liberian-flagged vessel, and passed them to the master of the SARAK (IMO 9226968). An email dated November 2024 from SEJ to the SARAK's vessel master included a photocopy of the FLEVES official stamp and a draft Q88 vessel questionnaire designed for insertion of false vessel information.

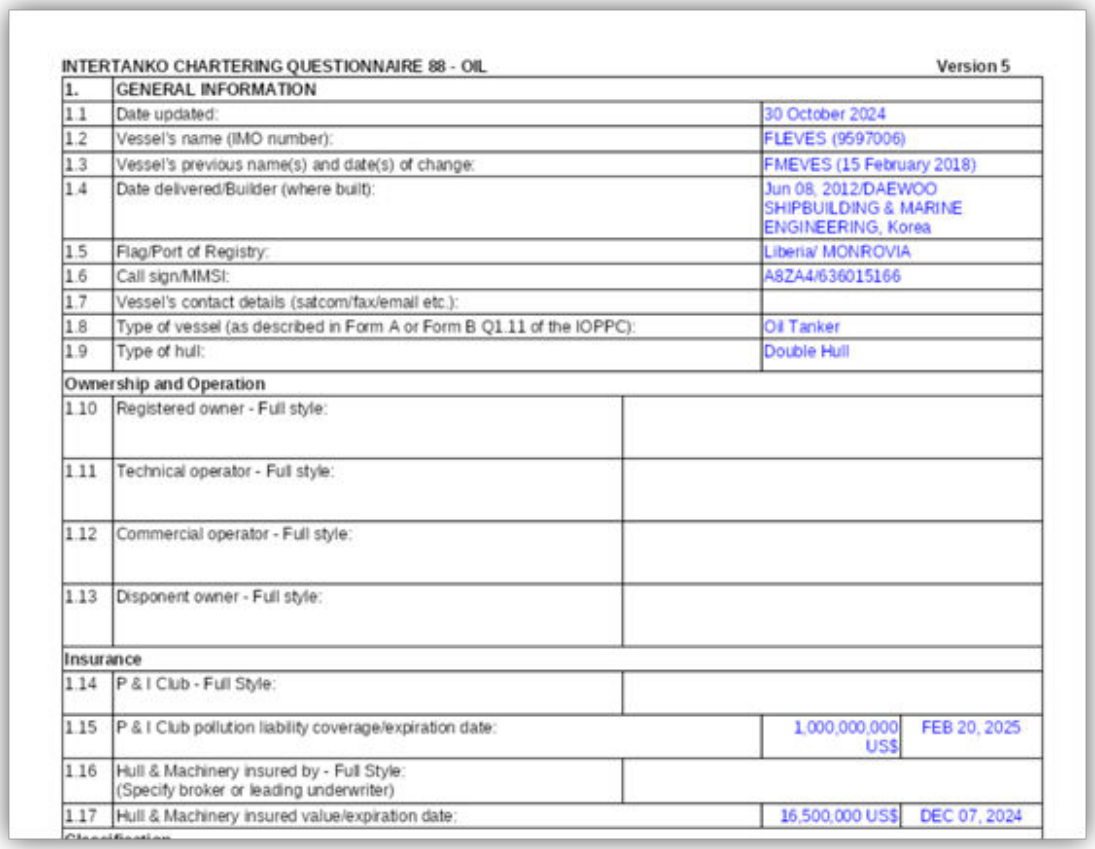
Dear sir,

Greetings,

Kindly find the fleves docs along the stamp scan to use for pri arrival docs to send for agent.

Best regards,

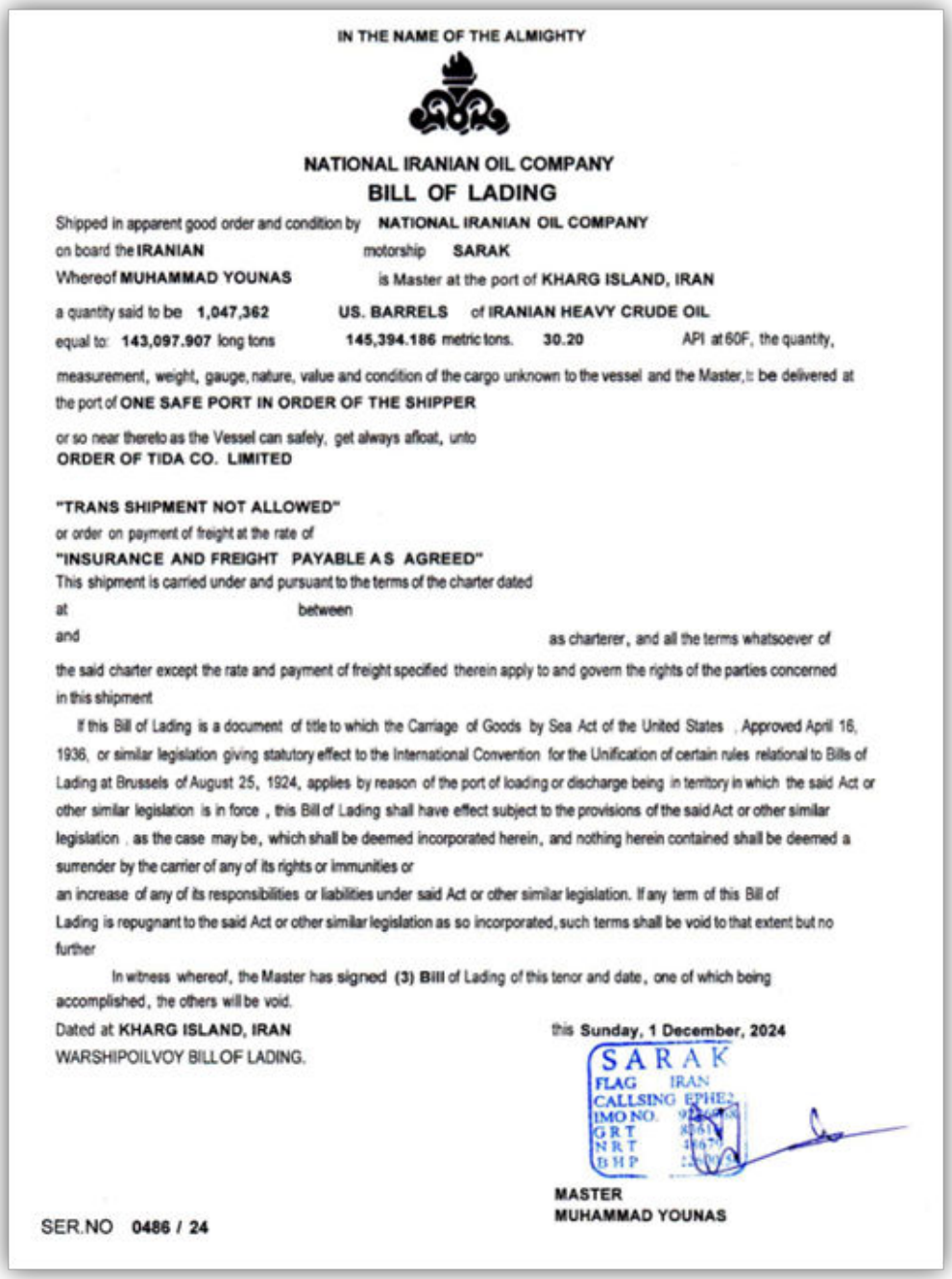
Ops Dep



INTERTANKO CHARTERING QUESTIONNAIRE 88 - OIL Version 5

1.	**GENERAL INFORMATION**		
1.1	Date updated:	30 October 2024	
1.2	Vessel's name (IMO number):	FLEVES (9597006)	
1.3	Vessel's previous name(s) and date(s) of change:	FMEVES (15 February 2018)	
1.4	Date delivered/Builder (where built):	Jun 08, 2012/DAEWOO SHIPBUILDING & MARINE ENGINEERING, Korea	
1.5	Flag/Port of Registry:	Liberia/ MONROVIA	
1.6	Call sign/MMSI:	A8ZA4/636015166	
1.7	Vessel's contact details (satcom/fax/email etc.):		
1.8	Type of vessel (as described in Form A or Form B Q1.11 of the IOPPC):	Oil Tanker	
1.9	Type of hull:	Double Hull	
Ownership and Operation			
1.10	Registered owner - Full style:		
1.11	Technical operator - Full style:		
1.12	Commercial operator - Full style:		
1.13	Disponent owner - Full style:		
Insurance			
1.14	P & I Club - Full Style:		
1.15	P & I Club pollution liability coverage/expiration date:	1,000,000,000 US$	FEB 20, 2025
1.16	Hull & Machinery insured by - Full Style: (Specify broker or leading underwriter)		
1.17	Hull & Machinery insured value/expiration date:	16,500,000 US$	DEC 07, 2024

Critically, the master of SARAK is listed as MUHAMMAD YOUNAS — the same name appearing as master of FLEVES. This is not document forgery in isolation; it is a coordinated human and paper trail replacement system.



IN THE NAME OF THE ALMIGHTY

NATIONAL IRANIAN OIL COMPANY

BILL OF LADING

Shipped in apparent good order and condition by **NATIONAL IRANIAN OIL COMPANY**
on board the **IRANIAN** motorship **SARAK**
Whereof **MUHAMMAD YOUNAS** is Master at the port of **KHARG ISLAND, IRAN**
a quantity said to be **1,047,362** **US. BARRELS** of **IRANIAN HEAVY CRUDE OIL**
equal to: **143,097.907** long tons **145,394.186** metric tons. **30.20** API at 60F, the quantity,
measurement, weight, gauge, nature, value and condition of the cargo unknown to the vessel and the Master, to be delivered at
the port of **ONE SAFE PORT IN ORDER OF THE SHIPPER**
or so near thereto as the Vessel can safely, get always afloat, unto
ORDER OF TIDA CO. LIMITED

"TRANS SHIPMENT NOT ALLOWED"
or order on payment of freight at the rate of
"INSURANCE AND FREIGHT PAYABLE AS AGREED"
This shipment is carried under and pursuant to the terms of the charter dated
at between
and as charterer, and all the terms whatsoever of
the said charter except the rate and payment of freight specified therein apply to and govern the rights of the parties concerned in this shipment

If this Bill of Lading is a document of title to which the Carriage of Goods by Sea Act of the United States, Approved April 16, 1936, or similar legislation giving statutory effect to the International Convention for the Unification of certain rules relational to Bills of Lading at Brussels of August 25, 1924, applies by reason of the port of loading or discharge being in territory in which the said Act or other similar legislation is in force, this Bill of Lading shall have effect subject to the provisions of the said Act or other similar legislation, as the case may be, which shall be deemed incorporated herein, and nothing herein contained shall be deemed a surrender by the carrier of any of its rights or immunities or
an increase of any of its responsibilities or liabilities under said Act or other similar legislation. If any term of this Bill of Lading is repugnant to the said Act or other similar legislation as so incorporated, such terms shall be void to that extent but no further

In witness whereof, the Master has signed **(3) Bill** of Lading of this tenor and date, one of which being accomplished, the others will be void.

Dated at **KHARG ISLAND, IRAN** this **Sunday, 1 December, 2024**
WARSHIPOILVOY BILL OF LADING.

SARAK
FLAG IRAN
CALLSING EPHE2
IMO NO. 9[illegible]
GRT [illegible]
NRT [illegible]
BHP [illegible]

MASTER
MUHAMMAD YOUNAS

SER.NO **0486 / 24**

NAME OF THE SHIP		M/T FLEVES		DATE	
NATIONALITY OF SHIP		LIBERIA		NOV 2024	
S.No.	FAMILY NAME/GIVEN NAME	RANK OR	NATIONALITY	DATE/PLACE OF BIRTH	
1	MUHAMMAD YOUNAS	MASTER	PAKISTAN	15.09.1982	SHANGLA,PAK
2	KHAN ZAHEER HAIDER	CH/OFF	INDIAN	07.05.1992	ALLAHABAD,UTTAR PRADESH

The same pattern applies to the SOBAR (IMO 9221970), operating under the cover of the PETALIDI (IMO 9529475). SEJ sent an email to SOBAR's master

titled "MT PETALIDI/procedure for documentation," attaching instructions for obtaining real-name stamps.

VESSEL FAKE NAME:	SOBAR PETALIDI

Dear sir,

Grettings,

Kindly please sign the docs as said procedure with fake stamp and find the real bl for real name stamp.

Best Regards,

IN THE NAME OF THE ALMIGHTY

NATIONAL IRANIAN OIL COMPANY

BILL OF LADING

Shipped in apparent good order and condition by NATIONAL IRANIAN OIL COMPANY
on board the IRANIAN motorship SOBAR
Whereof MUHAMMAD SHAFI is Master at the port of KHARG ISLAND, IRAN
a quantity said to be 1,052,797 US. BARRELS of IRANIAN HEAVY CRUDE OIL
equal to: 144,108.203 longtons 146,420.695 metric tons 29.90 API at 60F, the quantity, tons

measurement, weight, gauge, nature, value and condition of the cargo unknown to the vessel and the Master, to be delivered at the port of ONE SAFE PORT IN ORDER OF SHIPPER

or so near thereto as the Vessel can safely, get always afloat, unto
ORDER OF TIDA CO. LIMITED

"TRANS SHIPMENT NOT ALLOWED"
or order on payment of freight at the rate of
"INSURANCE AND FREIGHT PAYABLE AS AGREED"
This shipment is carried under and pursuant to the terms of the charter dated
at between
and as charterer, and all the terms whatsoever of the said charter except the rate and payment of freight specified therein apply to and govern the rights of the parties concerned in this shipment

If this Bill of Lading is a document of title to which the Carriage of Goods by Sea Act of the United States, Approved April 16, 1936, or similar legislation giving statutory effect to the International Convention for the Unification of certain rules relational to Bills of Lading at Brussels of August 25, 1924, applies by reason of the port of loading or discharge being in territory in which the said Act or other similar legislation is in force, this Bill of Lading shall have effect subject to the provisions of the said Act or other similar legislation, as the case may be, which shall be deemed incorporated herein, and nothing herein contained shall be deemed a surrender by the carrier of any of its rights or immunities or
an increase of any of its responsibilities or liabilities under said Act or other similar legislation. If any term of this Bill of Lading is repugnant to the said Act or other similar legislation as so incorporated, such terms shall be void to that extent but no further

In witness whereof, the Master has signed (3) Bill of Lading of this tenor and date, one of which being accomplished, the others will be void

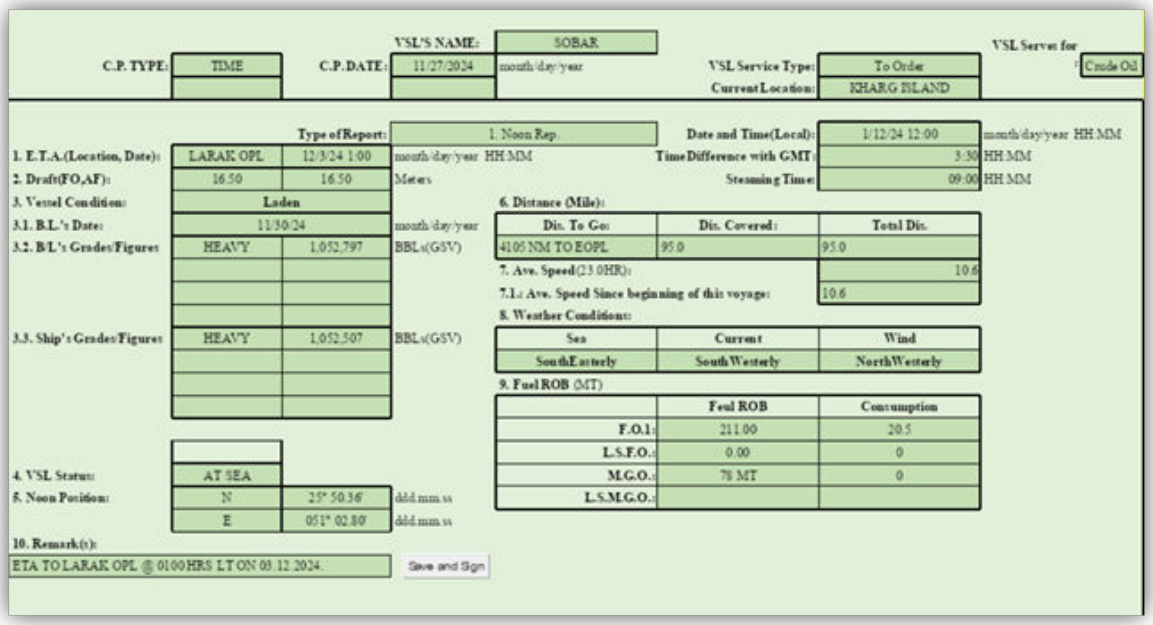
Dated at KHARG ISLAND, IRAN this Saturday, 30 November, 2024

WARSHIPOILVOY BILL OF LADING

MASTER
MT SOBAR

MASTER
MUHAMMAD SHAFI

SER.NO 0484 / 24



C.P. TYPE:	TIME	C.P. DATE:	11/27/2024	month/day/year	VSL'S NAME:	SOBAR	VSL Serves for: Crude Oil
					VSL Service Type:	To Order	
					Current Location:	KHARG ISLAND	

Type of Report:	1. Noon Rep.			Date and Time(Local):	1/12/24 12:00	month/day/year HH:MM	
1. E.T.A.(Location, Date):	LARAK OPL	12/3/24 1:00	month/day/year HH:MM	Time Difference with GMT:	3:30	HH:MM	
2. Draft(FO,AF):	16.50	16.50	Meters	Steaming Time:	09:00	HH:MM	
3. Vessel Condition:	Laden						
3.1. B/L's Date:	11/30/24		month/day/year				
3.2. B/L's Grades/Figures:	HEAVY	1,052,797	BBLs(GSV)				
3.3. Ship's Grades/Figures:	HEAVY	1,052,507	BBLs(GSV)				
4. VSL Status:	AT SEA						
5. Noon Position:	N	25° 50.36'	ddd.mm.ss				
	E	051° 02.80'	ddd.mm.ss				

6. Distance (Mile):

Dis. To Go:	Dis. Covered:	Total Dis.
4105 NM TO EOPL	95.0	95.0

7. Ave. Speed(23.0HR): 10.6

7.1. Ave. Speed Since beginning of this voyage: 10.6

8. Weather Conditions:

Sea	Current	Wind
SouthEasterly	SouthWesterly	NorthWesterly

9. Fuel ROB (MT)

	Feul ROB	Consumption
F.O.:	211.00	20.5
L.S.F.O.:	0.00	0
M.G.O.:	78 MT	0
L.S.M.G.O.:		

10. Remark(s):

ETA TO LARAK OPL @ 0100 HRS LT ON 03.12.2024.

Save and Sign

The actionable compliance implication is severe: a vessel owner may find their IMO number, flag documentation, Q88 records, and master's identity actively in use by a sanctioned Iranian hull, exposing them to OFAC designation under the 50 percent rule with no knowledge of the violation.

Flag-Hopping and Registry Exploitation. The SEJ fleet data shows Panama as the dominant flag of convenience, followed by Iran itself, then Guyana. The December 2025 OFAC action named vessels flagged in Palau, Panama, Barbados, Cook Islands, Jamaica, and the Marshall Islands. The February 2026 action added Comoros, Vanuatu, and Barbados. Each flag-hop resets the vessel's visible compliance profile. In one documented case, the tanker Bella 1, seized in the North Atlantic by US forces on 7 January 2026, changed its flag from Guyana to Russia during evasion, renamed itself Marinera, and smeared its registration details. The vessel evaded US tracking for eighteen days before a Monroe-led interdiction team boarded it 800 miles southeast of Iceland.

Shell Company Architecture. The ownership layer is deliberately designed to be impenetrable without sustained cross-jurisdictional investigation. The standard structure involves a single-purpose company registered in Panama or the Marshall Islands as nominal owner, a UAE-based ship management firm as operator, and an Iranian front company or exchange network collecting revenue. The December 2025 OFAC action identified this pattern across Arihant Shipping Inc. (Panama), Kurdos Shipping Inc. (Panama), Adonis Shipping Inc. (Marshall Islands), and Concord Shipping Inc. (Marshall Islands), all operating within the Persian Gulf under this layered structure.

Live Vessel Tracking: Confirmed Positions of OFAC-Designated Fleet

Real-time AIS tracking data, cross-referenced against the February 2026 OFAC designation list, confirms that a significant portion of the sanctioned fleet was actively transiting operational corridors at the time of or following their designation. The following positions were recorded:

- HOOT (IMO 9267962, Panama-flag, LPG tanker): Persian Gulf, 26.22°N / 55.65°E, speed 9.2 knots, last AIS report 6 February 2026. Owner: Poros Maritime Ventures S.A.
- OCEAN KOI (IMO 9255933, Barbados-flag): Persian Gulf, 26.24°N / 55.63°E, speed 14.5 knots, heading TERNEUZEN, last report 28 February 2026. Owner: Ocean Kudos Shipping Co Ltd.
- NORTH STAR (IMO 9299563, Barbados-flag): Laccadive Sea, 7.38°N / 77.35°E, speed 8.4 knots, last report 20 April 2026 — active movement as of the date of this report. Owner: Mistral Fleet Co Ltd.
- FELICITA (IMO 9167162, Comoros-flag): Laccadive Sea, 8.25°N / 76.72°E, speed 5.3 knots, last report 28 February 2026. Owner: Vast Marine Inc.
- ATEELA 1 (IMO 9548990, Iran-flag): Persian Gulf, 27.11°N / 56.30°E, speed 3.5 knots, last report May 2025. Owner: Behengam Tadbir Qeshm Shipping.
- ATEELA 2 (IMO 9549009, Iran-flag): Persian Gulf, 27.07°N / 56.28°E, speed 0 knots (anchored), last report October 2024. Owner: Behengam Tadbir Qeshm Shipping.
- NIBA (IMO 9046784, Palau-flag, 33 years old): Persian Gulf, 26.22°N / 55.65°E, speed 12.5 knots, last report 26 March 2026. Owner: Paros Maritime S.A.
- LUMA (IMO 9034690, Vanuatu-flag, 33 years old): Persian Gulf, 26.23°N / 55.64°E, speed 12.4 knots, last report 23 February 2026. Owner: Wansa Gas Shipping Co.
- REMIZ (IMO 9223344, Panama-flag): South China Sea, 1.86°N / 104.71°E, speed 0.4 knots, last report 24 December 2025. Owner: Goldwave Maritime Services Inc.
- DANUTA I (IMO 9193721, Palau-flag): Singapore Strait, 1.26°N / 104.17°E, speed 10.7 knots, last report 25 March 2026. Owner: Ithaki Maritime and Trading S.A.

- ALAA (IMO 9155341, Palau-flag): Gulf of Aden, 12.89°N / 48.42°E, speed 11.9 knots, last report 7 March 2026. Owner: Kaito Navigation SA.
- GAS FATE (IMO 9147394, Panama-flag): Persian Gulf, 26.24°N / 55.63°E, speed 14.3 knots, last report 27 February 2026. Owner: NYR Shipping Company.

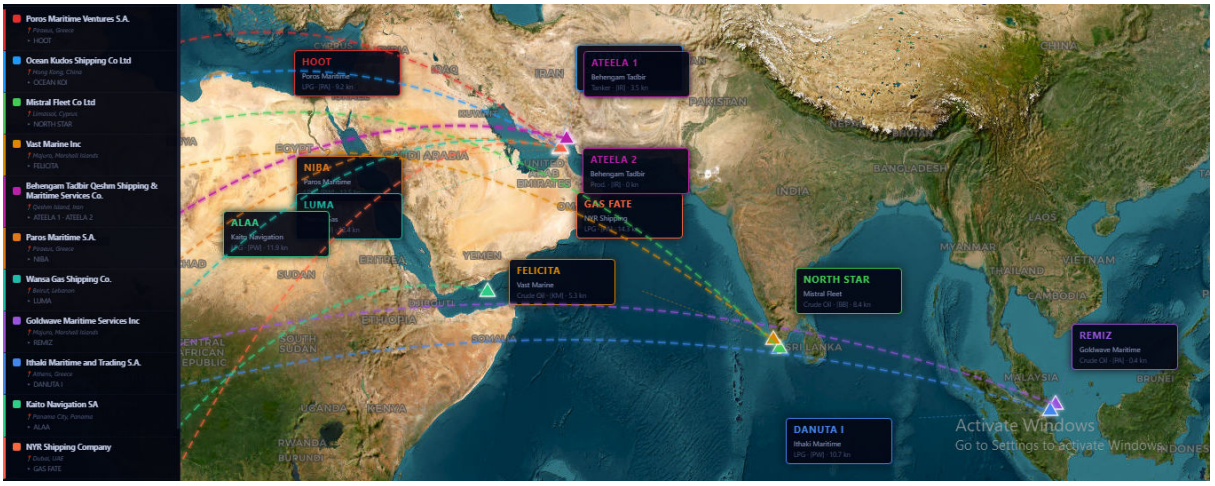
[Confirmed AIS positions of OFAC-designated shadow fleet vessels, February–April 2026. Clusters visible in Persian Gulf, Laccadive Sea, and Gulf of Aden]

E.O. 13902 Designations — Company Ownership of Blocked Vessels

Designated pursuant to Executive Order 13902 for operating in the petroleum sector of the Iranian economy · Vessels identified as blocked property of designated persons

#	Designated Company	Vessel(s) — Blocked Property	Jurisdiction	Designation Authority	Vessel Status
1	Poros Maritime Ventures S.A.	HOOT	Greece (Piraeus)	E.O. 13902	Blocked Property
2	Ocean Kudos Shipping Co Ltd	OCEAN KOI	Hong Kong, China	E.O. 13902	Blocked Property
3	Mistral Fleet Co Ltd	NORTH STAR	Cyprus (Limassol)	E.O. 13902	Blocked Property
4	Vast Marine Inc	FELICITA	Marshall Islands	E.O. 13902	Blocked Property
5	Behengam Tadbir Qeshm Shipping and Maritime Services Company	ATEELA 1 & ATEELA 2	Iran (Qeshm Island)	E.O. 13902	Blocked Property
6	Paros Maritime S.A.	NIBA	Greece (Piraeus)	E.O. 13902	Blocked Property
7	Wansa Gas Shipping Co.	LUMA	Lebanon (Beirut)	E.O. 13902	Blocked Property
8	Goldwave Maritime Services Inc	REMIZ	Marshall Islands	E.O. 13902	Blocked Property
9	Ithaki Maritime and Trading S.A.	DANUTA I	Greece (Athens)	E.O. 13902	Blocked Property
10	Kaito Navigation SA	ALAA	Panama	Vessel blocked*	Blocked Property
11	NYR Shipping Company	GAS FATE	UAE (Dubai)	Vessel blocked*	Blocked Property

** Kaito Navigation SA and NYR Shipping Company are not listed among the nine companies formally designated pursuant to E.O. 13902 in this action, but their associated vessels (ALAA and GAS FATE respectively) are identified as blocked property of previously designated persons.*

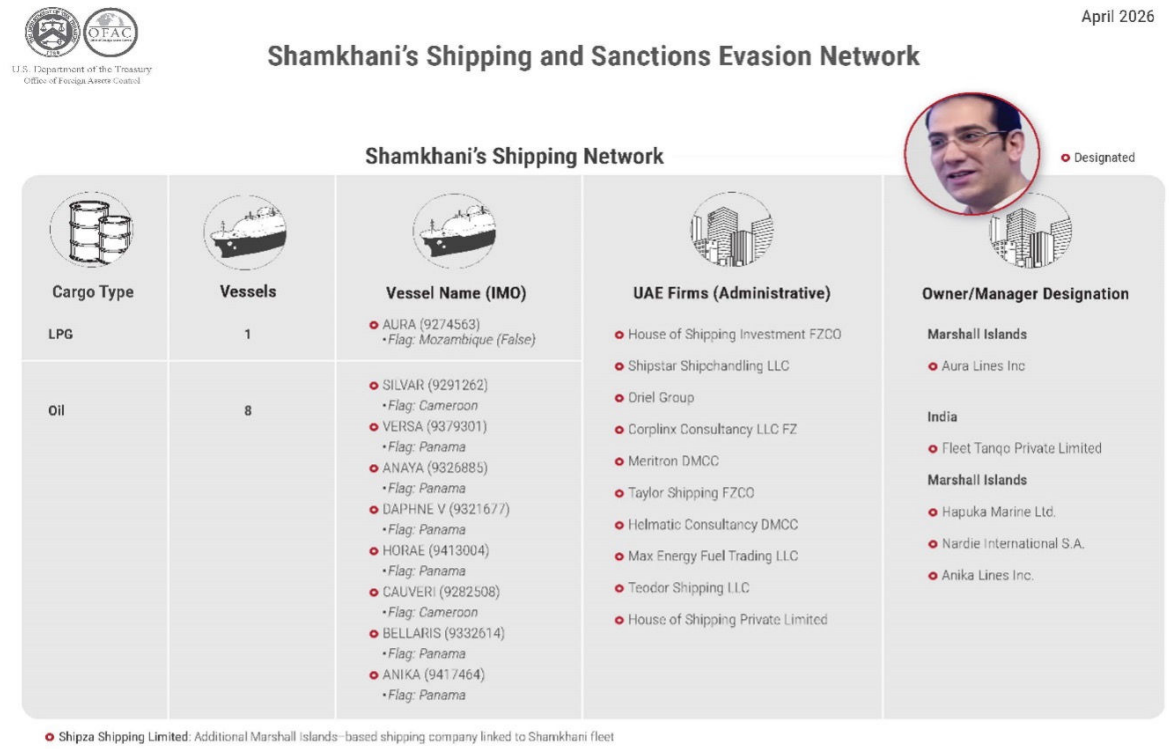


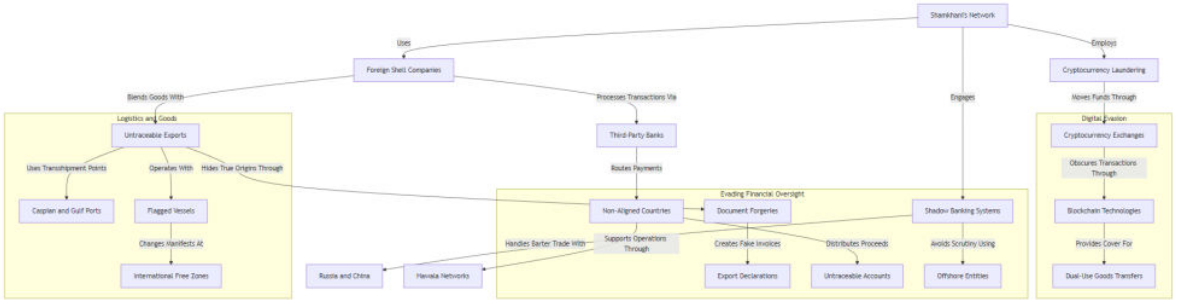
[Owner-to-vessel network map: OFAC February 2026 designated entities linked to their blocked vessels by operating company, flag, and last-known trajectory. Note routing lines from Persian Gulf toward South China Sea and Indian Ocean delivery corridors]

The age profile of this fleet is operationally significant. NIBA and LUMA are both 33 years old, operating well beyond standard commercial tanker life expectancy. ALAA is 28 years old. GAS FATE is 27 years old. These vessels are uninsurable in Western markets, deliberately so — their age eliminates them from P&I Club coverage, forcing reliance on sanctioned or opaque insurers such as Maritime Mutual, which was itself under investigation for insuring $18.2 billion in Iranian cargo. For underwriters, a vessel over 20 years old, flagged in Palau, Panama, Comoros, or Vanuatu, clustered in the Persian Gulf with last-known position near Fujairah anchorage, should be treated as presumptively shadow-fleet-affiliated until proven otherwise.

1.3 Named Networks — Prioritised Threat Actors

The Shamkhani Shipping Empire. Mohammad Hossein Shamkhani, son of deceased former National Security Council Secretary Ali Shamkhani, controls what OFAC describes as a multi-billion dollar Iranian and Russian petroleum sales empire. OFAC's July 2025 action — its largest single Iran designation since the Trump administration revived maximum pressure — covered fifteen shipping companies, 52 vessels, twelve individuals, and 53 entities, with estimated revenues of $1 billion channelled to the Iranian regime. The April 2026 "Economic Fury" action built on this, adding the following network entities:





Oriel Group (UAE): the administrative umbrella for all Shamkhani shipping and commodity operations.

Corplinx Consultancy LLC FZ (UAE): uses legitimate-looking web domains to disguise financial and corporate operations of the network.
House of Shipping Investment FZCO (UAE) and its Indian subsidiary House of Shipping Private Limited: direct shipping arm.
Meritron DMCC (UAE): vessel procurement front, having contributed tens of millions of dollars toward two new South Korean-built vessels ordered through 2025–2026 to replace designated assets.
Shipstar Shipchandling LLC (UAE): provisions vessels, enabling them to remain crewed and operational. Also identified in the Anonymous #OpIran WikiIran leak.
Taylor Shipping FZCO (formerly Lazar Shipping, UAE): managed the sanctioned YUG vessel during Iranian commodity deliveries to East Asia on behalf of SEJ.
Shipza Shipping Limited (Marshall Islands): linked to sanctioned vessels STAR (IMO 9436484) and TAVA 4 (IMO 9292151).
Fleet Tanqo Private Limited (India): manages HORAE, VERSA, ANAYA, DAPHNE V, and SILVAR, which collectively transported more than 20 cargoes of Russian petroleum products in 2025.

The Shamkhani network's November 2024 Anonymous leak — published via @anonymousopiran with 156,000 followers — exposed internal operating documents, company addresses, vessel names (including a Disney-character naming scheme: Pinocchio, Simba, Goofy, Dragon Ball), and procurement email channels. The documents were assessed as high credibility by NightTeam OSINT, given direct overlap with the July 2025 OFAC designation. The Telegram screenshots published within that leak show coordination between Draco Buren Shipping (1 Maritime Square, Singapore), Crios Shipping (Maze Tower, Sheikh Zayed Road, Dubai), Koban Shipping (Conrad Office Tower, Dubai), and Sidus Marine (West Connect Building, Singapore; Tehran office in Lavasan). OFAC confirmed all four as core Shamkhani network companies.

Hossein Shamkhani is the eldest son of Ali Shamkhani, who along with his family, each of whom owns several apartments worth several billion, owns several large shipping companies. According to his Facebook information, he is a graduate of the Lebanese American University.

Mr. Hossein Shamkhani, in the guise of Mr. Ali Rahbar Madani, as the owner of the ships and manager of numerous parts of the complex, engages in rent-seeking, corruption, and money laundering.

The ship "Kabul", owned by the Admiral Company, owned by the sons of Ali Shamkhani, Secretary of the Supreme Security Council of Iran, was stopped in India in 1400 due to document violations.

The lack of documentation and sailing under the flag of another country, along with Ali Shamkhani's tweet, indicate that this ship was linked to the issue of circumventing sanctions. Shamkhani wrote that we will sacrifice our lives and reputation to heal the wound of "sanctions." The unsaid will be left for later.

shamkhani.pdf

650.5 KB

Open with

Hossein Shamkhani, the eldest son of Ali Shamkhani, owns several large shipping companies along with his family, each of which owns several apartments worth several thousand billion.

Mr. Hossein Shamkhani, in the guise of Mr. Ali Rahbar Madani, is engaged in corruption, rent-seeking, and money laundering as the owner of the ships and the manager of numerous parts of the complex.

The full details of this corruption chain were first revealed by Anonymous. All information about this corruption chain will be sent to relevant agencies to stop this chain.

> We Are Legion
> We Are Anonymous
> We Don't Forget
> We Don't Forgive
> Expect Us!
> #OpIran

Their most important company is DRACO BUREN. They use this company to ship many ships to the United States. send

DRACO BUREN TRANSPORT COMPANY

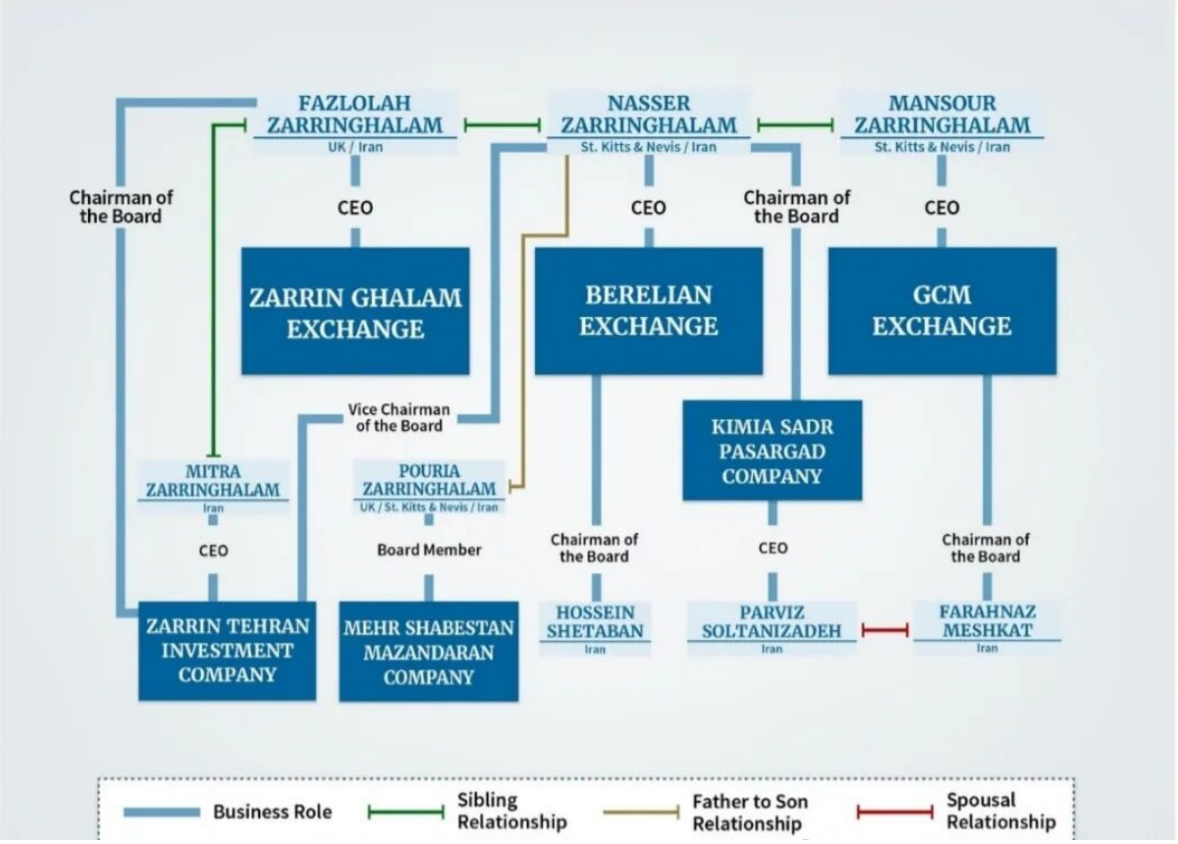
buy1@draco-buren.com This company's support email

draco-buren.com website address

draco-buren.cloudfleetmanager.com Fleet Management System Website Address

1 maritime square, #09-59, harbourfront centre, Singapore-099253 Address

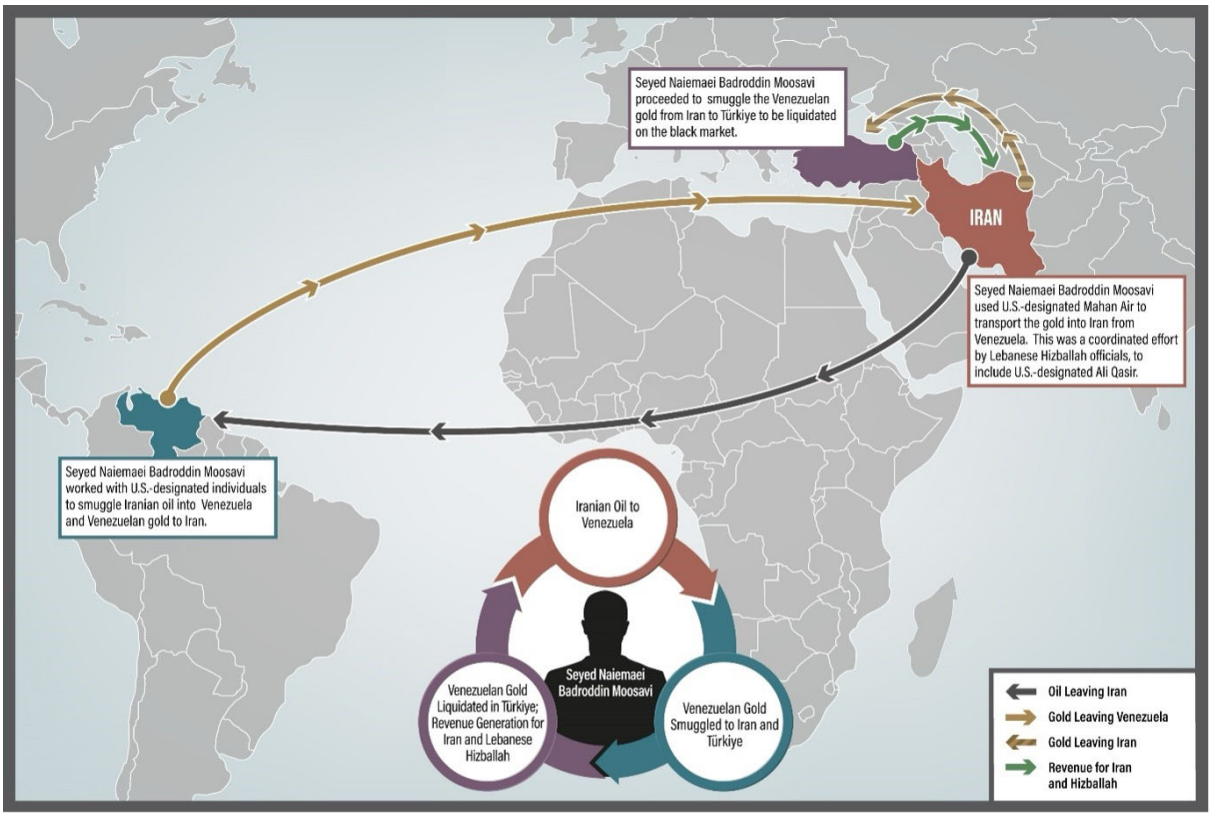
The Zarringhalam Shadow Banking Network. The Zarringhalam brothers — Mansour, Nasser, and Fazlolah — operate a currency exchange and front company network across UAE and Hong Kong that has laundered approximately $1 billion for the Iranian regime, per the June 2025 OFAC/State Department action. The brothers control GCM Berelian and Zarrin Ghalam exchange houses, and a network of shell trading companies in UAE free zones and Hong Kong. These entities receive oil sale proceeds from Iranian exporters and convert them to USD through forged documents and agent-line banking relationships that exploit US correspondent accounts. FinCEN identified approximately $9 billion in potential Iranian shadow banking activity transiting US correspondent accounts in 2024 alone.

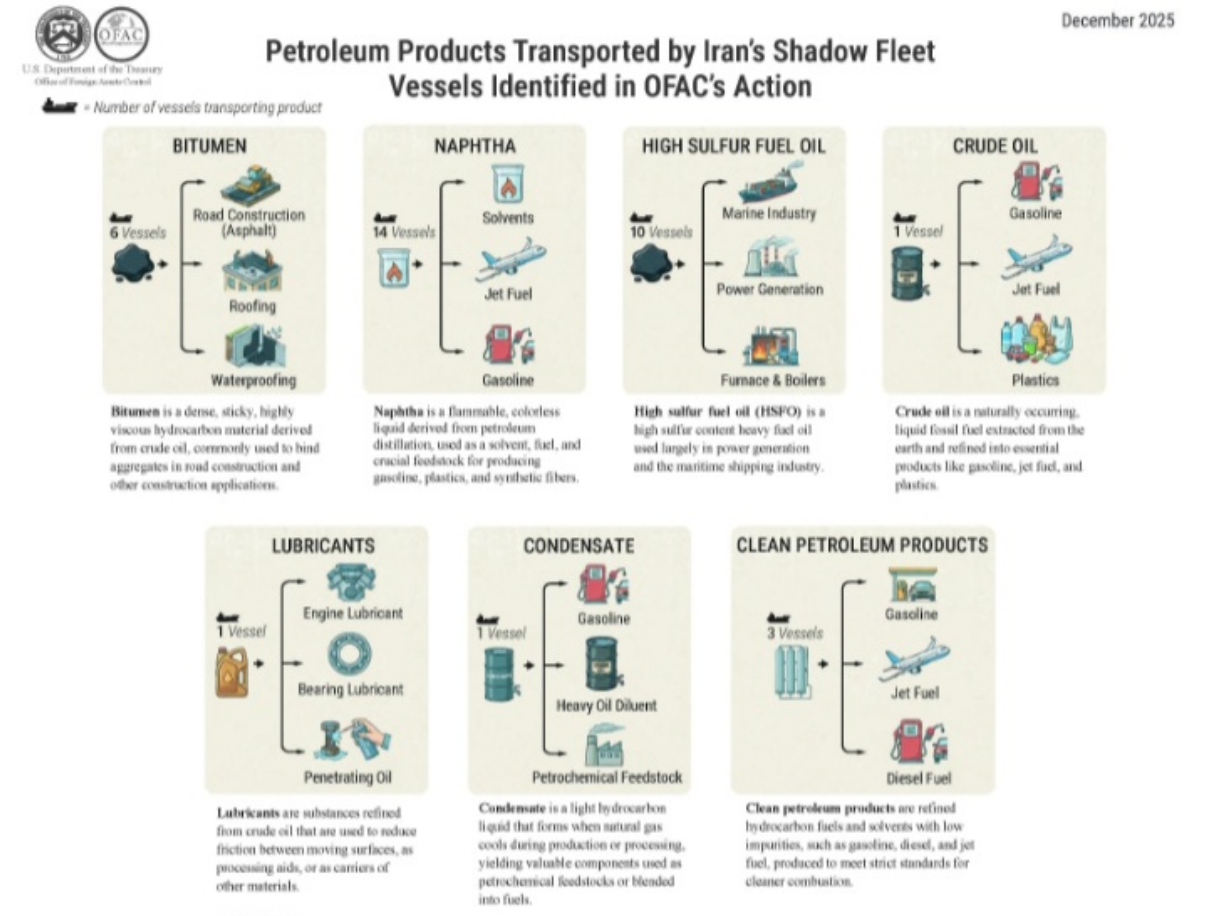


The Tehran Loop Financial Architecture. Per Nitishastra's analysis, Iranian oil revenues are not simply sold and repatriated. IRGC energy credits are swapped for vostro credits in mid-tier Omani banks. These credits are bundled into collateralised synthetic obligations that reach London repo desks as high-quality collateral backing short-term loans. Dubai initiates and disguises flows, Hong Kong restructures and redistributes them, London legitimises and reintegrates them, and Europe consolidates and converts them into assets. The system combines hawala networks with blockchain transaction routing and AI-driven layering to stay ahead of jurisdiction-siloed enforcement. The practical result is that Iranian oil money is already embedded in the City of London's collateral base.

The Moosavi Oil-for-Gold Scheme. The April 2026 Economic Fury action revealed a previously undocumented Iran-Venezuela-Hezbollah triangular financing loop. Seyed Naiemaei Badroddin Moosavi, an IRGC-QF-linked Iranian national and Hezbollah financier, smuggled Iranian oil into Venezuela under the Maduro regime in exchange for gold procured at below-market rates. The gold was then transported on US-designated Mahan Air to Hezbollah members in Tehran, smuggled to Turkey, and sold for operational financing. Moosavi worked directly with US-designated narcotics trafficker Tarek El Aissami and

sanctioned shipping facilitator Viktor Artemov (a Ukrainian citizen with IRGC-QF links) to execute these transfers using STS operations, AIS spoofing, and zombie tankers.





TankerTrackers documented in June 2025 that the maximum pressure campaign had not reduced global dark fleet tonnage but had instead caused a fleet reshuffle, with vessels previously assigned to Russian oil rotating into Iranian transport roles as designations created temporary gaps. This whack-a-mole dynamic is precisely what the Middle East Institute described as the core structural problem: enforcement raises operating costs and slows flows but does not eliminate them, because the pool of available vessels exceeds the designation rate.

[TankerTrackers, 12 June 2025: The global dark fleet exceeded 1,200 vessels by mid-2025. Tankers previously moving Russian oil rotated into Iranian oil transport as maximum pressure designations created supply gaps in the Russian evasion network]

1.4 The Ballistic Missile Financing Loop

The February 2026 OFAC action explicitly connected the shadow fleet revenue stream to Iran's weapons procurement architecture, establishing the closed loop between petroleum exports and weapons development. Oje Parvaz Mado Nafar Company (Mado), previously designated for supporting the IRGC, manufactures engines for the Shahed-131 and Shahed-136 UAVs. Three Turkey-based companies — Utus Gumrukleme, Arya Global, and Altis Tekstil — served as financial intermediaries for Mado, originating transfers exceeding $1 million for sensitive machinery acquisition. Additionally, Adak Pargas Pars (Iran) and Mostafa Roknifard Prime Choice General Trading LLC (UAE) facilitated procurement of sodium perchlorate, a ballistic missile solid-propellant precursor, on behalf of Parchin Chemical Industries. Four QAI employees — Mohammad Abedini, Mehdi Zand (Russia deployments), Mehrdad Jafari, and

Ebrahim Shariatzadeh (Venezuela deployments) — traveled on behalf of Qods Aviation Industries to provide UAV technical support to Russia and Venezuela respectively, documenting the direct link between shadow fleet revenue and front-line weapons capability.

Key table — Networks Supplying Iran's Ballistic Missile and ACW Programs:

Entity	Jurisdiction	Role	Designated Authority
Oje Parvaz Mado Nafar (Mado)	Iran	UAV engine production (Shahed-131/136)	E.O. 13382
Utus Gumrukleme	Turkey	Financial intermediary for Mado; hundreds of thousands USD	E.O. 13382
Arya Global Gida	Turkey	Financial intermediary; >$1M in Mado machinery purchases	E.O. 13382
Altis Tekstil Makina	Turkey	Financial transactions for Mado procurement	E.O. 13382
Adak Pargas Pars	Iran	Sodium perchlorate procurement for PCI	E.O. 13382
MRPCG Trading (Roknifard)	UAE	Sodium perchlorate facilitation	E.O. 13382
Qods Aviation Industries (QAI)	Iran	Mohajer-series UAV design and export to Russia, Venezuela	E.O. 13949
IRGC ASF SSJO	Iran	Ballistic missile R&D; flight test launches	E.O. 13382

实体/人员名称 (Name)	类型 (Type)	注册地/国籍 (Jurisdiction)	关联船只/备注 (Vessels/Notes)
Hatem Elsaid Farid Ibrahim Sakr	个人	埃及 (Egypt)	影子船队的关键推动者，与伊朗军方幌子公司 Sahara Thunder 有关联
Phoenix Ship Management FZE	实体	阿联酋 (UAE)	管理船只: NEBULA DRIFT, AETHER SAIL, TIDAL RHYTHM, VOYAGER HAVEN
Arihant Shipping Inc.	实体	巴拿马 (Panama)	拥有船只: ARIHANT
Kurdos Shipping Inc.	实体	巴拿马 (Panama)	拥有船只: KURDOS, KURDOS II, KURDOS III
Adonis Shipping Inc	实体	马绍尔群岛 (Marshall Islands)	拥有船只: KASSIA
Concord Shipping Inc.	实体	马绍尔群岛 (Marshall Islands)	拥有船只: MAJESTY
Rukbat Marine Services Co	实体	印度 (India)	拥有船只: FLORA DOLCE
Aleah Shipping Inc	实体	英属维尔京群岛 (BVI)	拥有船只: DIANA
J M A Shipping Inc.	实体	巴拿马 (Panama)	拥有船只: J MA
S M A Shipping Inc.	实体	巴拿马 (Panama)	拥有船只: S MA
MKA Shipping Inc	实体	马绍尔群岛 (Marshall Islands)	拥有船只: MKA (此前曾运输俄罗斯来源的石脑油)

Golden Gate Ship Management	实体	印度 (India)	拥有船只: AUROURA
Darya Shipping Private Limited	实体	印度 (India)	运营船只: RAMYA
Sinostar Marine Group Limited	实体	马绍尔群岛 (Marshall Islands)	拥有船只: FOSHAN
Hemera Lines Inc.	实体	马绍尔群岛 (Marshall Islands)	拥有船只: HEMERA
Agape Shipping Inc	实体	马绍尔群岛 (Marshall Islands)	拥有船只: NOMIKI
Maruti Shipping Inc.	实体	马绍尔群岛 (Marshall Islands)	拥有船只: MARUTI
Everest Sea Navigation SA	实体	利比里亚 (Liberia)	拥有船只: GOLDEN EAGLE
Red Sea Ship Management LLC	实体	阿联酋 (UAE)	Sakr 拥有的公司。关联船只: SKYLIGHT, KHADIGA, INTAN PREMIER
High Seas Petroleum LLC	实体	阿联酋 (UAE)	Sakr 拥有的公司 (前身为 Petrofleet Energy Trading LLC)
Qatrat Alnada Almasi Ship Management L.L.C	实体	阿联酋 (UAE)	关联船只: SEA WISE, SEAMULL, SEA ROCK, SEA CITRINE VI (涉及停靠胡塞武装港口)

NOTE: All entity and vessel names are listed in English. Chinese-language annotations in the above tables carry the following substantive information not otherwise captured in English:

MKA Shipping Inc. — The notation "此前曾运输俄罗斯来源的石脑油" indicates that the vessel MKA **previously transported Russian-origin naphtha**, suggesting the vessel's sanctions exposure extends beyond Iranian petroleum and may reflect a broader pattern of sanctions evasion involving multiple jurisdictions.

Qatrat Alnada Almasi Ship Management L.L.C. — The notation "涉及停靠胡塞武装港口" confirms that vessels under this company's management — SEA WISE, SEAMULL, SEA ROCK, and SEA CITRINE VI — have made **documented stops at Houthi-controlled ports in Yemen**. This is significant as it establishes a direct operational link between Iran's oil export shadow fleet and the logistical support network of a U.S.-designated terrorist organization, the Houthis (Ansarallah).

Column headers — For reference: 类型 = Type · 注册地/国籍 = Jurisdiction · 关联船只/备注 = Associated Vessels/Notes · 实体 = Entity · 个人 = Individual.

1.5 The China Teapot Refinery Node

The most consequential single destination node for Iranian oil exports is China's independent refinery sector, commonly known as teapot refineries, concentrated in Shandong Province. These refineries purchase the majority of Iranian crude exports and have become the primary commercial anchor of the shadow fleet's revenue cycle.

OFAC's first teapot designation under NSPM-2 was Shandong Shouguang Luqing Petrochemical Co. (March 2025), sanctioned for purchasing and refining hundreds of millions of dollars of Iranian crude. The second action (April 2025) designated Shandong Shengxing Chemical Co. for purchasing more than a billion dollars' worth of Iranian crude, including from an IRGC-Qods Force front company. The third action (May 2025) added Hebei Xinhai Chemical Group and three Shandong Province terminal operators for facilitating delivery of hundreds of millions of dollars' worth of Iranian oil. A fourth teapot refinery, Shandong Jincheng Petrochemical Group, was designated in October 2025. By the sixth round of NSPM-2 sanctions (April 2025), the State Department had also designated Huaying Huizhou Daya Bay Petrochemical Terminal Storage Co. for knowingly receiving approximately one million barrels of Iranian crude in January 2025.

The enforcement pattern follows a predictable architecture: sanctioned vessels conduct STS transfers with newly-designated tankers (for example, the LAMD, formerly TAI HE, transported eight million barrels of Iranian oil to multiple Chinese locations since mid-2024, while the SKADI conducted multiple STS operations with already-sanctioned vessels including CATALINA 7 and NATALINA 7). Each designation closes one node while Iran's network substitutes replacement vessels and terminal relationships.
Foreign financial institutions face secondary sanctions risk for knowingly facilitating significant transactions for any designated teapot or terminal entity. The practical consequence is that any bank, insurer, or trading counterparty whose clients include Chinese buyers of Iranian crude — even absent direct knowledge of the origin — is within the secondary sanctions perimeter documented in the December 2025 OFAC and FinCEN advisories.

U.S. Department of the Treasury
Office of Public Affairs

Press Release: **FOR IMMEDIATE RELEASE**
April 16, 2025

Contact: press@treasury.gov

Treasury Increases Pressure on Chinese Importers of Iranian Oil

WASHINGTON – Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) is designating a China-based independent "teapot" refinery **Shandong Shengxing Chemical Co., Ltd.** for its role in purchasing more than a billion dollars' worth of Iranian crude oil, including from a front company for Iran's Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF). OFAC is also imposing additional sanctions on several companies and vessels responsible for facilitating Iranian oil shipments to China as part of Iran's "shadow fleet."

"Any refinery, company, or broker that chooses to purchase Iranian oil or facilitate Iran's oil trade places itself at serious risk," said Secretary of the Treasury Scott Bessent. "The United States is committed to disrupting all actors providing support to Iran's oil supply chain, which the regime uses to support its terrorist proxies and partners."

Today's action is being taken pursuant to Executive Order (E.O.) 13902, which targets Iran's petroleum and petrochemical sectors, and is OFAC's second action against a teapot refinery that has purchased Iranian crude oil. This also marks the sixth round of sanctions targeting Iranian oil sales since the President issued National Security Presidential Memorandum 2 (NSPM-2), instituting a campaign of maximum economic pressure on Iran.

SECTION 2: INSIDER RECRUITMENT AND PORT LOGISTICS FRAUD

2.1 UAE as the Primary Transshipment Node

The UAE's free-zone architecture — particularly Jebel Ali, Fujairah, and the Dubai Investment Park — provides the legal and logistical infrastructure for cargo manifest falsification. Phoenix Ship Management FZE (UAE) managed four vessels — NEBULA DRIFT, AETHER SAIL, TIDAL RHYTHM, and VOYAGER HAVEN — that transported hundreds of thousands of barrels of Iranian condensate, bitumen, and naphtha in 2025 under a UAE operational identity. The Shamkhani network's Shipstar Shipchandling LLC operates from Plot 597-4228, Dubai Investment Park-2, providing provisions directly to shadow fleet vessels calling at UAE ports.

The UAE transshipment architecture has expanded beyond crude oil to cover LPG supply chains penetrating South Asian markets previously considered lower-risk. Slogal Energy DMCC (UAE), designated in the October 2025 OFAC action, purchased Iranian LPG that was delivered to Sri Lanka and Bangladesh across 2024 and 2025, with multiple shipments reaching end users documented by OFAC. The GAS DIOR (IMO 9379404, Panama-flagged) delivered over 17,000 metric tons of Iranian LPG to Bangladesh in early 2025, with additional deliveries tied to now-sanctioned supplier Octane Energy FZCO. This routing through Bangladesh and Sri Lanka represents the southward extension of the UAE transshipment node, exploiting the limited enforcement capacity of smaller South Asian port authorities.

The Somali financial infrastructure penetration documented in Section 2.3 has a parallel precedent in the March 2026 Dahabshiil and Telesom case. Both Somali money transfer businesses reportedly received fuel deliveries from a US Treasury-sanctioned Iranian Revolutionary Guard vessel — demonstrating that sanctions-designated vessels are not merely evading detection at commercial ports but are actively conducting commercial delivery relationships with legitimate regional financial entities. Any financial institution processing payments or remittances for entities that interact with sanctioned IRGC-linked fuel suppliers is within the Zarringhalam network's correspondent banking exposure pattern.

2.2 Indian Networks

Three India-based companies were identified in the December 2025 OFAC action: Rukbat Marine Services Co (managing FLORA DOLCE, which transported millions of barrels of Iranian fuel oil since April 2025), Golden Gate Ship Management (operating AUROURA for Iranian naphtha and condensate), and Darya Shipping Private Limited (operating RAMYA from September 2025).

The April 2026 action added Fleet Tanqo Private Limited (India) and House of Shipping Private Limited (India, a direct subsidiary of the UAE Shamkhani umbrella). India has also in February 2026 seized three Iranian oil tankers sanctioned by the US, indicating growing bilateral enforcement cooperation. However, India's dual exposure — it imports more than 60 percent of its oil from the Middle East — means its port officials operate at the intersection of the highest enforcement pressure and the highest economic vulnerability.

2.3 FinCEN Warning Signs as an Insider Recruitment Red Flag Framework

The June 2025 FinCEN advisory is operationally useful as a recruitment detection tool. High-risk indicators that port officials or shipping agents have been compromised include: transport documents where the maritime database shows an Iran port call but the submission does not; vessels claiming IMO numbers that belong to different or scrapped ships; shipments described as "Malaysian blend oil" transiting via Southeast Asia with AIS anomalies; wire transfers to companies whose stated business does not match recipient counterparties (oil receivables going to electronics companies); and multiple companies formed simultaneously with similar ownership and address structures. These last two patterns are specific to the Zarringhalam network's UAE and Hong Kong operations and should be treated as primary screening criteria.

The Dahabshiil and Telesom case from March 2026 illustrates the port-level penetration risk. Both Somali money transfer businesses reportedly received fuel deliveries from a US Treasury-sanctioned Iranian Revolutionary Guard vessel. This case demonstrates that sanctions-designated vessels are not simply detected at major commercial ports — they are actively conducting business relationships with legitimate regional financial infrastructure, creating compliance exposure for any institution in their payment chain.

2.4 The Alang Beach Dollar Laundromat

[TankerTrackers, 2 January 2026: At least 14 OFAC-sanctioned tankers, 12 Iran-linked, scrapped at Alang Beach, India during 2025. One VLCC arrived with AIS switched off. Sales proceeds converted to USD, flowing directly back to vessel owners]

The Alang Beach ship-breaking yard in Gujarat, India represents a previously underdocumented cash-out mechanism for the shadow fleet. When a sanctioned vessel has exhausted its operational utility — through age, multiple designations, or excessive enforcement exposure — it is sailed to Alang with AIS disabled, scrapped, and sold for steel. The USD proceeds of that sale flow back to the vessel's nominal owner — typically a Marshall Islands or Panama single-purpose company — where they are converted into clean capital outside any sanctions enforcement framework. At least fourteen OFAC-sanctioned tankers, twelve of them Iran-linked, underwent this process during 2025 alone. One of them was a Very Large Crude Carrier that arrived with its AIS transponder off. The beach, in the words of TankerTrackers, has become a dollar laundromat. This mechanism closes the full sanctions-evasion lifecycle: vessel operates under false identity, generates oil revenue routed through shadow banking, is eventually designated, then is liquidated through a

legitimate industrial process in a non-sanctioning jurisdiction for hard currency. Compliance implication for GRC teams: Any financial institution processing payments for ship-recycling transactions at Alang, Chittagong, or Gadani involving vessels with histories of AIS anomalies, flag changes, or opaque ownership should treat those transactions as potentially facilitating the final-stage cash-out of a shadow fleet asset.

SECTION 3: FINANCIAL OFF-RAMPS — DARK WEB SENTIMENT AND CYBER INFRASTRUCTURE

3.1 Sanctions-as-a-Service and Underground Market Pricing

The shift from entity-based to behaviour-based sanctioning documented in the December 2025 to April 2026 OFAC actions (targeting AIS manipulation, shell company architecture, and STS activity patterns rather than waiting for confirmed cargo) has driven the shadow fleet to seek more sophisticated camouflage. The Wikilran leak confirms that SEJ actively operates a systematic vessel-identity procurement system, which implies an upstream market for stolen maritime documentation. The procurement emails show SEJ obtaining original vessel stamps, Q88 questionnaire blanks, and master identity records — a document procurement pipeline that requires either insider access to vessel management systems or an active black market for maritime credentials.

The Kpler compliance analysis from January 2026 documents that AIS spoofing, shell-company ownership structures, and false insurance certificates collectively constitute a commoditised evasion toolkit used consistently across the shadow fleet ecosystem. The predictable pre-designation behavioral pattern — false positioning, flag changes, dark STS activity — visible months before enforcement action suggests that detection tools have not yet eliminated the supply side of this market.

3.2 Crypto and Stablecoin Off-Ramps

The JINSA March 2026 analysis confirms that following the January 2026 designation of Muslim Brotherhood branches as terrorist organizations, Hamas's financial network pivoted to crypto assets and hawala networks. The IRGC's broader sanctions-evasion infrastructure, per both FinCEN and the Zarringhalam network profile, increasingly routes through TRON blockchain stablecoins. The FATF's targeted report on stablecoins and unhosted wallets (Group 3 source) is directly relevant here — unhosted wallets used in

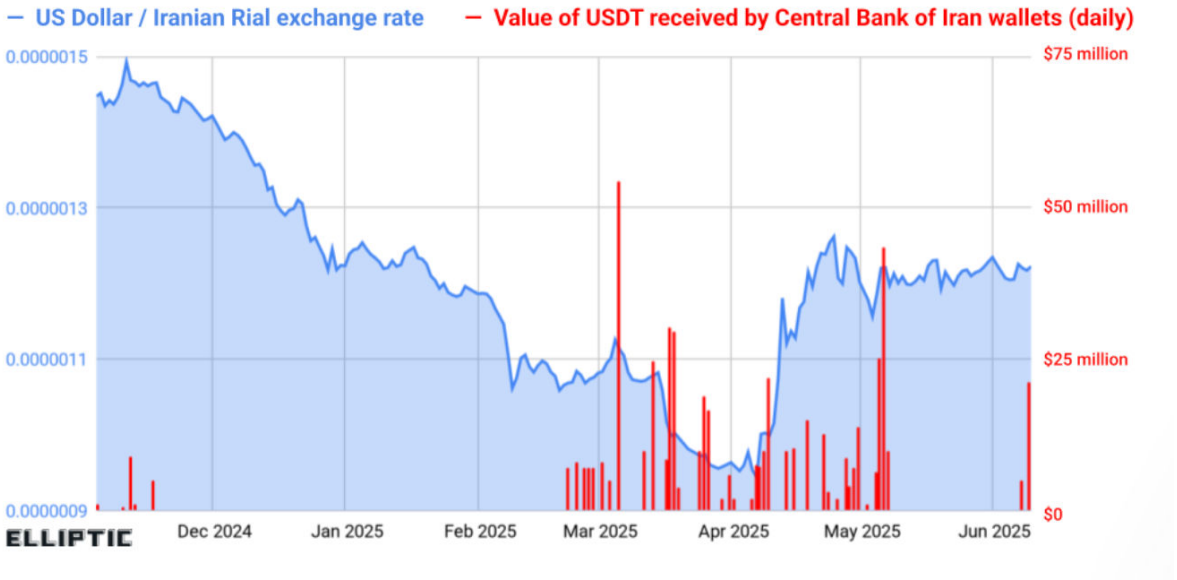
combination with peer-to-peer exchanges allow Iranian-linked entities to convert oil proceeds into USD-equivalent assets without touching the SWIFT system. The Nitishastra Tehran Loop analysis further confirms that AI-driven transaction routing is being used to layer crypto flows across jurisdictions to defeat pattern-matching detection.

The TRM Labs 2026 Crypto Crime Report documents that IRGC-linked addresses accounted for over 50 percent of all value received by Iranian entities in Q4 2025, moving more than $3 billion to support regional militia networks, facilitate oil sales, and procure dual-use equipment. Iran's illicit activity was overwhelmingly concentrated in USDT stablecoins on the TRON blockchain, reflecting the asset's liquidity, low transaction costs, and compatibility with broker-mediated settlement networks. This preference for TRON-based USDT is operationally significant: it means that transaction monitoring systems calibrated primarily to Ethereum-chain or Bitcoin activity will systematically undercount Iranian sanctions evasion flows.

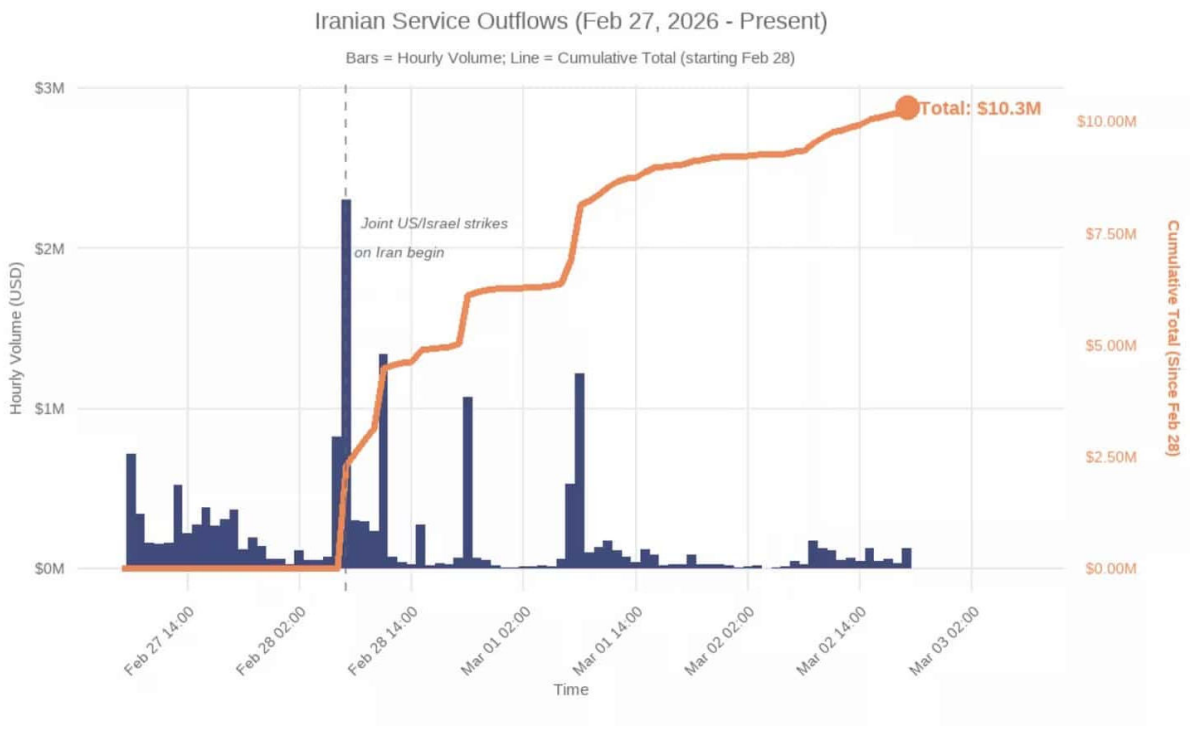
The most structurally significant TRM finding is the identification of two cryptocurrency exchanges incorporated in the United Kingdom — Zedcex Exchange Ltd and Zedxion Exchange Ltd — that processed hundreds of millions of dollars in USDT stablecoin transactions while functioning as offshore financial infrastructure linked to the IRGC. OFAC designated both entities in January 2026 in the first-ever designation of IRGC-linked digital asset exchanges. TRM analysis confirmed that one of the exchanges processed approximately $1 billion in funds linked to IRGC-associated activity across 2023 through 2025, accounting for roughly 56 percent of its total transaction volume — peaking at 87 percent in 2024. On-chain evidence shows that over $10 million in USDT was transferred directly from a wallet attributable to Zedcex to addresses controlled by US-designated Houthi financier Sa'id al-Jamal. UK authorities subsequently moved to dissolve both companies.

The operational model uncovered by TRM represents a structural escalation: rather than money laundering through a series of wallets, the IRGC operated exchange-branded digital asset infrastructure directly embedded in global stablecoin markets. The use of UK corporate registration to access that global stablecoin ecosystem — combining Tron's liquidity with the reputational cover of a UK-incorporated entity — is precisely the kind of jurisdictional arbitrage the Tehran Loop financial architecture was designed to exploit. A senior Iranian financier, Babak Morteza Zanjani — already notorious for laundering billions in oil revenue in an earlier designation — is identified by TRM as the corporate trail link reconstructing his networks through digital asset rails. OFAC

designated Zanjani alongside the two exchanges in January 2026.
The Chainalysis 2026 Crypto Crime Report corroborates the TRM findings, documenting that sanctioned entities transacted $154 billion through illicit crypto addresses in 2025, with stablecoins accounting for 84 percent of such activity. Iran's crypto ecosystem reached $7.78 billion in 2025, growing faster than the prior year — a figure comparable to the entire GDP of smaller sovereign states. Iran legalized crypto mining in 2019, allowing licensed operators to use subsidized electricity in exchange for selling mined Bitcoin to the central bank, creating a state-managed mining infrastructure that estimates put at between two and five percent of global Bitcoin mining power.



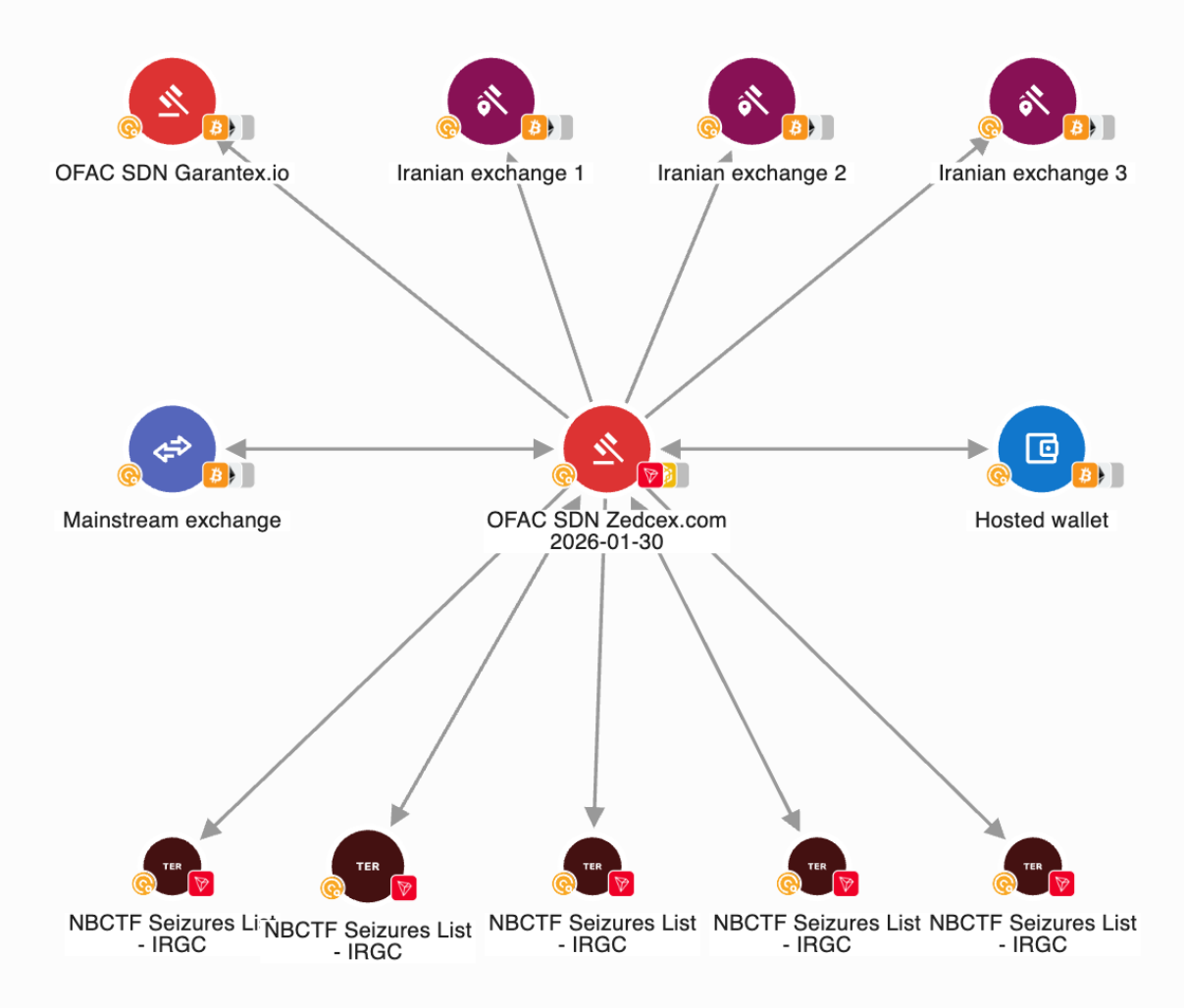
[Iran's $USDT value (Elliptic)]



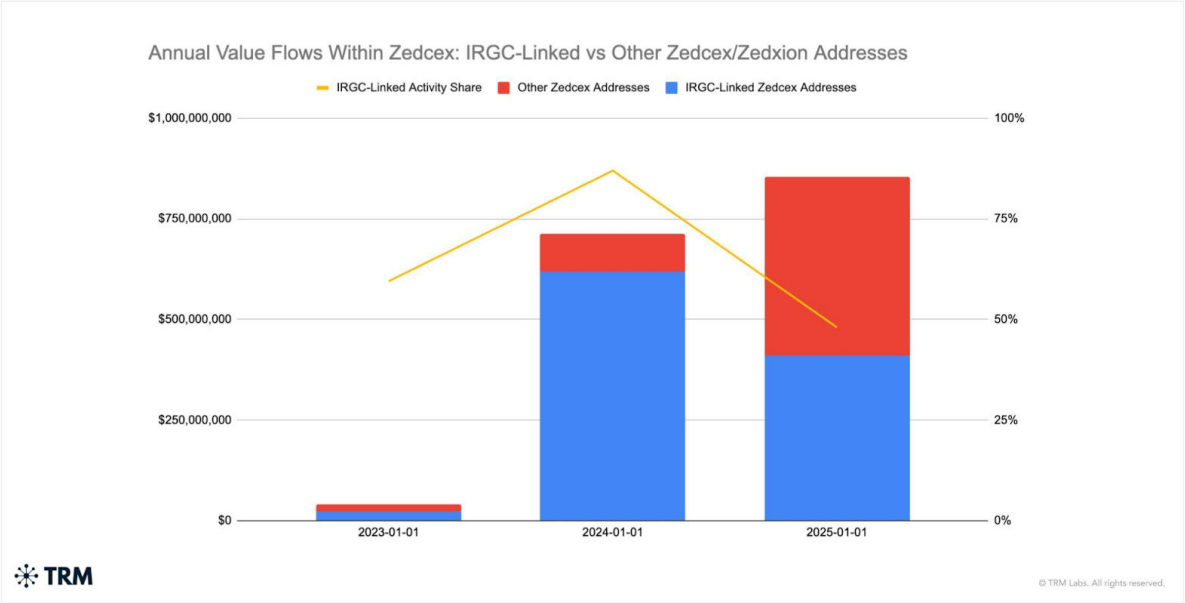
Iran's Crypto Economy at a Glance

Metric	Figure
Total ecosystem size (2025)	$7.78 billion
IRGC share of on-chain inflows (Q4 2025)	50%+
IRGC value received (2025)	$3 billion+
Volume drop after Feb 28 strikes	~80%
Primary stablecoin used	USDT (USDT-toman pair)
BTC price reaction to strikes	Fell to ~$64,000, partial recovery
ZEC 1-year performance	+500%+
BTC ETF inflow snap (March 3)	$458 million single day

[WazirX report]



[The ChainAnalysis Reactor graph below shows a sample of Zedcex's interaction with IRGC counterparties, as well as Iranian exchanges, other sanctioned entities, and compliant services]



Today's OFAC action against Zedcex, Zedxion, Babak Zanjani, and associated wallet infrastructure represents a major disruption of IRGC-linked stablecoin financing activity. It also reflects the next phase of crypto sanctions enforcement: identifying, attributing, and disrupting illicit financial infrastructure before it becomes normalized at scale.

3.3 Hacktivist and Cyber Threat to Price-Cap Infrastructure

The Anonymous #OpIran doxing campaign against the Shamkhani network demonstrates that non-state information warfare actors are actively targeting the financial legitimacy infrastructure of the shadow fleet. The November 2025 leak published via @anonymousopiran was timed to follow the July 2025 OFAC designation, amplifying reputational damage and potentially accelerating secondary enforcement action by exposing company addresses, email channels, and vessel names to public scrutiny. The IRGC-affiliated APT groups (APT33, APT34, Charming Kitten) have documented histories of targeting maritime and financial infrastructure. With the April 2026 naval blockade now operational, the incentive for cyber disruption of insurance clearance systems, shipping registry databases, and correspondent banking infrastructure has increased substantially.

3.4 The Insurance Market as the Primary Blockade Mechanism

[Gas prices aren't rising because the Strait of Hormuz is blocked by war. It's blocked by the insurance markets and speculators betting that the region will stay chaotic]

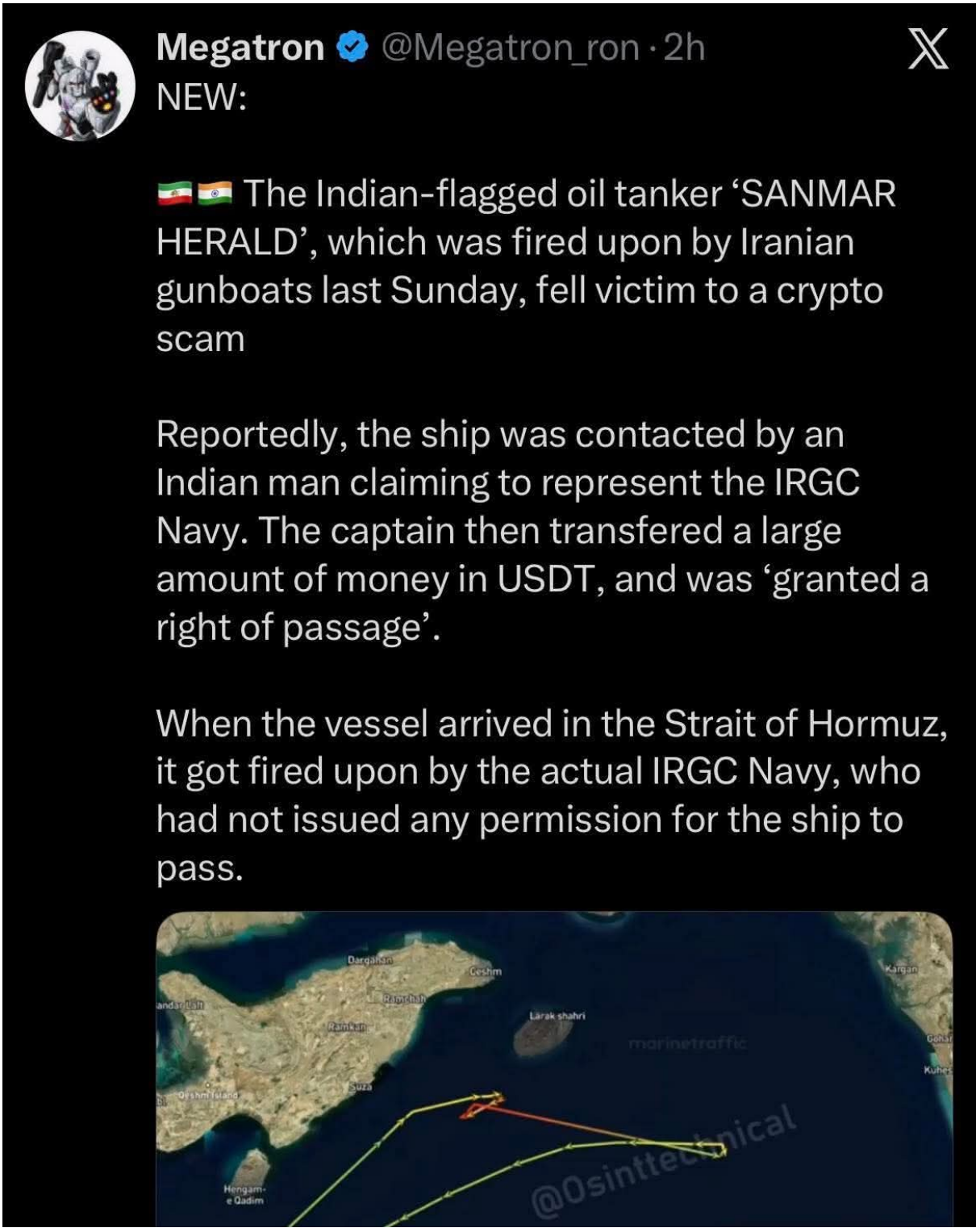
This observation, despite its informal sourcing, captures a mechanism that the JINSA "Scared Strait" report confirmed through formal analysis. The physical blockade and the insurance blockade are operating as parallel but distinct systems, and the insurance mechanism is arguably more durable. JINSA's March 2026 assessment stated directly that insurance coverage remains technically available but that even with President Trump's proposal to cushion rising rates through US government-backed reinsurance, these policies are finding few takers. Shippers are refusing to transit not primarily because of kinetic interdiction but because of the perceived risk of losing vessels and crews — a perception the insurance market is actively pricing and amplifying rather than absorbing.

The practical enforcement consequence is that the US naval blockade does not need to physically intercept every vessel to achieve economic closure. The withdrawal of war-risk coverage creates a commercial blockade that runs

parallel to the military one. Shadow fleet operators with no Western insurance exposure — precisely the vessels documented throughout this report — are therefore the only actors capable of continued transit, which is why TankerTrackers documented sanctioned tankers entering and departing the blockade zone with ease (Section 1.1, Image 3) while commercially insured vessels stopped entirely. The blockade has inadvertently created a market structure where sanctioned actors have a competitive advantage over legitimate shippers, because they have already been excluded from the insurance system that is now enforcing the shutdown.

For maritime underwriters this is the core actionable finding from this subsection: the war-risk premium surge is not simply a pricing adjustment — it is a de facto secondary sanctions mechanism. Any underwriter reinstating coverage for Persian Gulf transits without conducting vessel identity verification against the WikiIran and OFAC datasets is potentially providing the only commercial input these sanctioned operators lack.

3.5 Sanctions-as-a-Service: The IRGC Navy Impersonation Crypto Scam



[Indian-flagged tanker SANMAR HERALD fired upon by Iranian gunboats after captain transferred large amount of USDT to an individual claiming to represent the IRGC Navy, who had promised right of passage. The actual IRGC Navy had issued no such permission]

This incident shows significant dark web / fraud intelligence finding because it documents in open source, a live Sanctions-as-a-Service product actively being sold at the vessel level in real time during the blockade. The mechanism is as follows: a threat actor, likely monitoring vessel AIS and distress communications, contacts vessels approaching the Strait claiming IRGC Navy authority. They offer a right of passage in exchange for USDT payment — an untraceable, instant stablecoin transfer that requires no banking infrastructure and leaves no correspondent account trail. The captain of SANMAR HERALD complied, transferring a large USDT amount. The vessel then entered the Strait and was immediately fired upon by the actual IRGC Navy, which had issued no passage permission.

The product being sold — Hormuz passage clearance — has a real buyer at a real price point, denominated in USDT, collected by an actor who may or may not have IRGC affiliation but is exploiting the information asymmetry of the blockade environment. Several conclusions follow:

First, the price of passage clearance is now a live market with active price discovery, not a theoretical construct. The USDT denomination means payments are instantaneous, pseudonymous, and cross-border — meeting the FinCEN stablecoin risk criteria exactly.

Second, this is insider recruitment at the vessel level. The scam requires knowledge of which vessels are approaching, their flag state, their captain's communication channel, and the degree of desperation created by insurance withdrawal. That targeting profile implies either AIS monitoring capability or a port agent intelligence feed from UAE or Omani coastal facilities.

Third, regardless of whether this specific actor is IRGC-affiliated, the IRGC benefits from the chilling effect. Every vessel that receives such a contact — whether it pays or not — faces a credible threat that slows transit decisions and amplifies the commercial blockade effect documented in Section 3.4.

3.6 The Hormuz Toll Booth: Crypto as War Finance

The most structurally consequential financial development of the active conflict phase is Iran's formalization of the Strait of Hormuz as a crypto-denominated toll collection point. Since mid-March 2026, the IRGC has been charging oil tankers and LNG carriers up to $2 million each to pass through the Strait, accepting payment in Bitcoin, USDT, or Chinese yuan. The toll is calculated at approximately $1 per barrel of crude cargo. A fully loaded very large crude carrier hauling two million barrels therefore pays $2 million before it clears the waterway.

The fee structure was confirmed publicly on April 8, 2026, by Hamid Hosseini, a spokesperson for Iran's Oil, Gas and Petrochemical Products Exporters' Union, who told the Financial Times that tankers must email Iranian authorities with cargo details, after which Iran instructs crews on payment in digital currencies. Hosseini explicitly stated that Bitcoin was the preferred method: "Once the email arrives and Iran completes its assessment, vessels are given a few seconds to pay in bitcoin, ensuring they can't be traced or confiscated due to sanctions." Empty tankers transit free. Fully laden vessels must comply.

Iran formalized the arrangement through the Strait of Hormuz Management Plan, codified by the Iranian parliament on March 30–31, 2026. According to Lloyd's List, the IRGC has imposed a controlled corridor close to the Iranian coastline, between the islands of Qeshm and Larak. Ships hoping to use the pre-approved route must submit to a vetting scheme managed through a series of Iran-affiliated intermediaries outside Iran, providing full details of vessel ownership, cargo manifests, crew lists, and destination, and communicate those details to the IRGC Navy's Hormozgan Provincial Command for sanctions screening and what has been described as geopolitical vetting.

At 21 million barrels of oil per day transiting the Strait — prior to the blockade — the theoretical toll revenue at $1 per barrel generates an estimated $21 million daily, or approximately $630 million per month from oil tankers alone. Including LNG carriers, estimates from TRM Labs and other analytics providers suggest revenues of $600 to $800 million monthly, with an annualized ceiling approaching $7.6 billion at full continuous operation. This transforms the Strait from a logistical chokepoint into a recurring revenue stream denominated outside any dollar-based financial system.

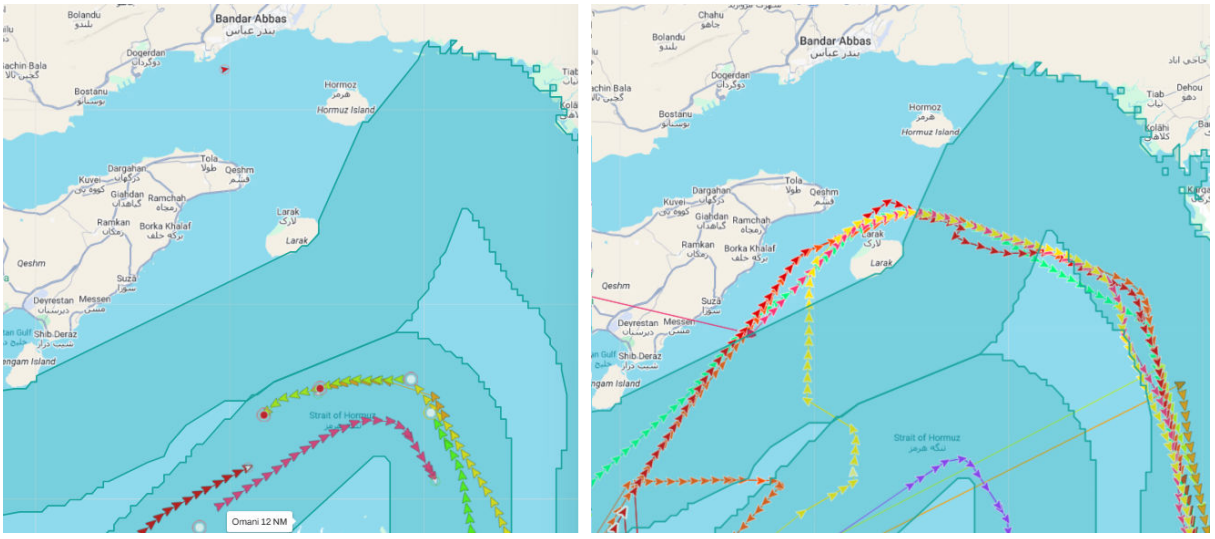
The operational procedure, documented by Bloomberg and Lloyd's List, involves vessel operators negotiating fees through IRGC-linked intermediaries, submitting documentation up to 96 hours in advance, and then receiving a one-time passcode and an IRGC escort upon confirmed payment. Since March 13, 2026, all tracked transits through the Strait have used the IRGC-controlled corridor; no transits via the normal pre-war route have been documented since March 15.

Multiple governments — India, Pakistan, Iraq, Malaysia, and China — are understood to have discussed vessel transit plans directly with Tehran, with Iran's foreign minister Abbas Araghchi conducting direct calls with counterparts in Malaysia, China, Egypt, South Korea, and India. According to the Indian government, no fees are being paid for Indian ships, suggesting that diplomatic intervention provides passage without payment for politically

acceptable flag states, while commercial vessels lacking such diplomatic cover face the full toll regime.

The crypto toll system has directly spawned a secondary fraud market. Fraudsters impersonating IRGC officials have been demanding Bitcoin and USDT from shipping companies whose vessels are stranded in the Strait, as documented by Greek maritime risk management firm MARISKS. The SANMAR HERALD incident (Section 3.5) represents the most documented case, but the broader scam ecosystem is generating fraudulent passage demands ranging from hundreds of thousands to millions of dollars in Bitcoin or USDT. The scam works because it mirrors a real policy — the IRGC's actual toll collection using the same assets and similar processes — creating an information asymmetry that is nearly impossible for vessel operators to resolve in real time.

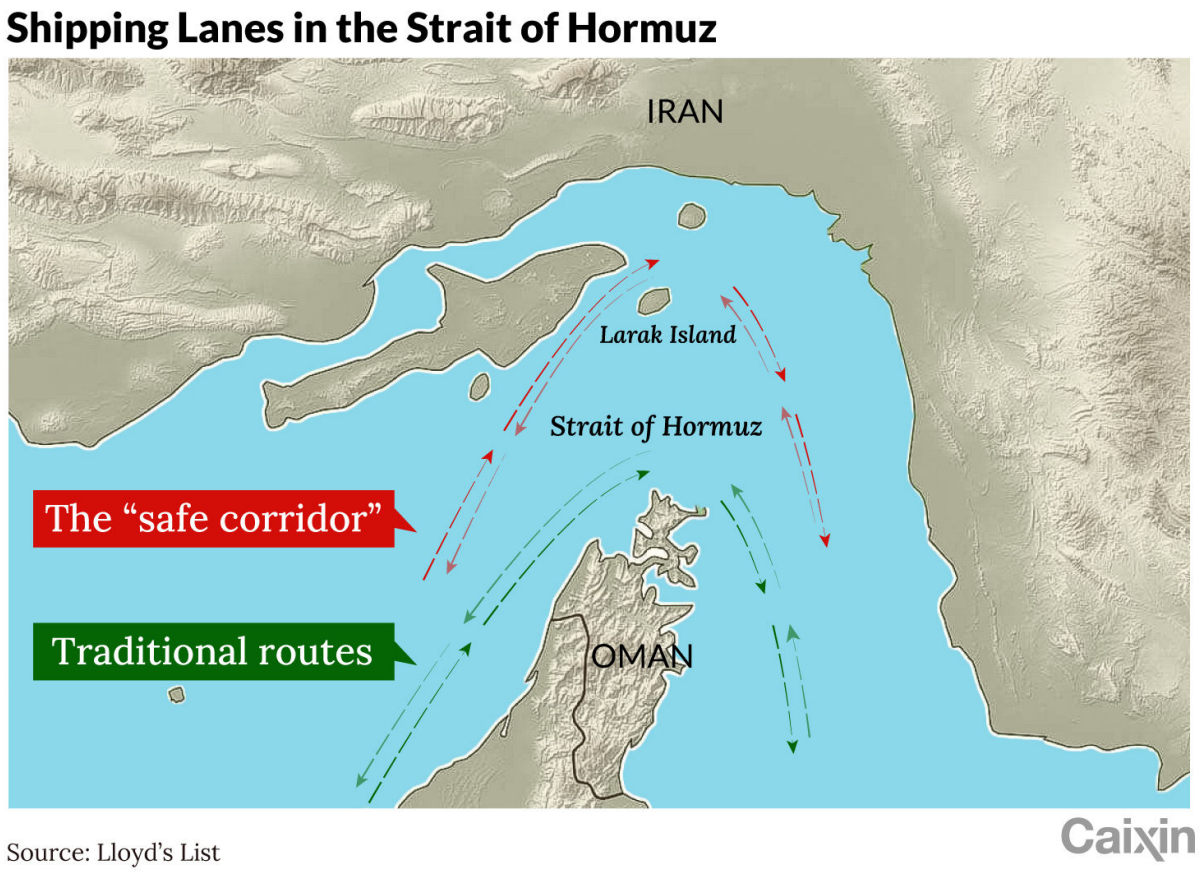
The Iran foreign policy analyst Hamidreza Gholamzadeh (Diplo House) has assessed that Iran is using Hormuz control as leverage to structurally accelerate de-dollarisation of global energy trade, conditioning passage on yuan-denominated oil settlement at an estimated $3 trillion annual cost to the US dollar system. The crypto toll formalizes this in practice: each $2 million USDT or Bitcoin payment is a transaction that permanently exits the dollar correspondent banking system and enters Iran's sanctions-evasion financial architecture. At scale, the cumulative effect is a structural compression of petrodollar recycling into US Treasuries — the financial off-ramp sabotage documented in Section 4.3, now occurring via operational commercial enforcement rather than theoretical geopolitical negotiation.



[Left: snapshot of pre-war tanker traffic through the strait

Right: Vessels (mostly bulkers) looping around Larak Island and through

Iran's territorial waters. All bulkers in the right image — except for the one in purple taking the normal route through SOH — came from Iran]



Source: Lloyd's List

[The "safe corridor," established on March 13, runs between Larak and Qeshm islands in the Iranian territorial waters, moving ships away from the deeper, central shipping lanes in the Strait of Hormuz. Iran uses this corridor vetting vessels passage and reportedly, in some cases, collecting fees]

THE HILL

Instaread

Iran will require ships passing through the Strait of Hormuz to pay the cryptocurrency equivalent of $1 per barrel of oil on board during the two-week ceasefire with the U.S, a key figure told the Financial Times.

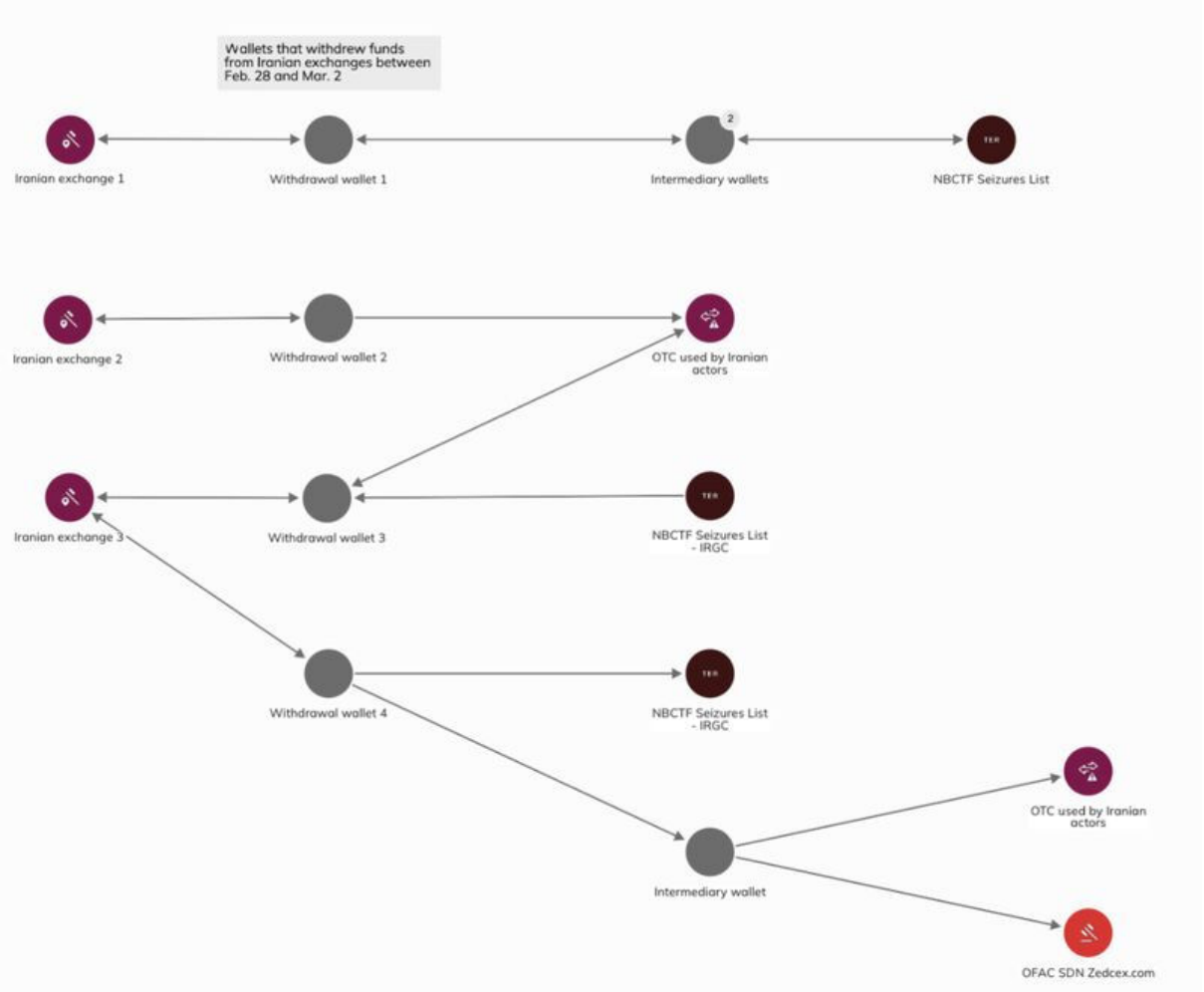
Hamid Hosseini, a spokesperson for Iran's Oil, Gas and Petrochemical Products Exporters' Union, which works with Iran's government, told the Financial Times about the requirement on Wednesday.

He said that it will cost $1 per barrel of oil and that ships need to email Iranian authorities about what they are carrying.

"Once the email arrives and Iran completes its assessment, vessels are given a few seconds to pay in bitcoin, ensuring they can't be traced or confiscated due to sanctions," Hosseini told the newspaper.

He added that the measures are being put in place to make sure weapons are not carried through the strait.

ChainAnalysis says: It's still too soon to estimate how much of Iranian crypto activity this week is IRGC-related, but some of the wallets that withdrew funds during the initial spike in outflows from Iranian exchanges have historical exposure to known IRGC wallets, indicating that at least a portion of the activity following the strikes could represent Iranian state movement of funds.



3.7 GPS and AIS Warfare: The Invisible Blockade

The kinetic blockade of the Strait of Hormuz has been accompanied by a parallel electronic warfare campaign that has made the Strait operationally unnavigable for commercially insured vessels independent of the physical threat environment. On February 28, 2026, the first day of Operation Epic Fury, GPS interference disrupted the navigation systems of more than 1,100 commercial ships across UAE, Qatari, Omani, and Iranian waters within 24 hours. Windward AI identified at least 21 new AIS jamming clusters across the region in that single operational period.

Dryad Global confirmed in a February 19, 2026 advisory that commercial maritime traffic in the Gulf of Oman and Strait of Hormuz was already experiencing elevated risks of GPS jamming and AIS spoofing directly linked to ongoing Iranian military exercises, including the IRGC Navy's "Smart Control of the Strait of Hormuz" drill initiated around February 16. The interference aligns

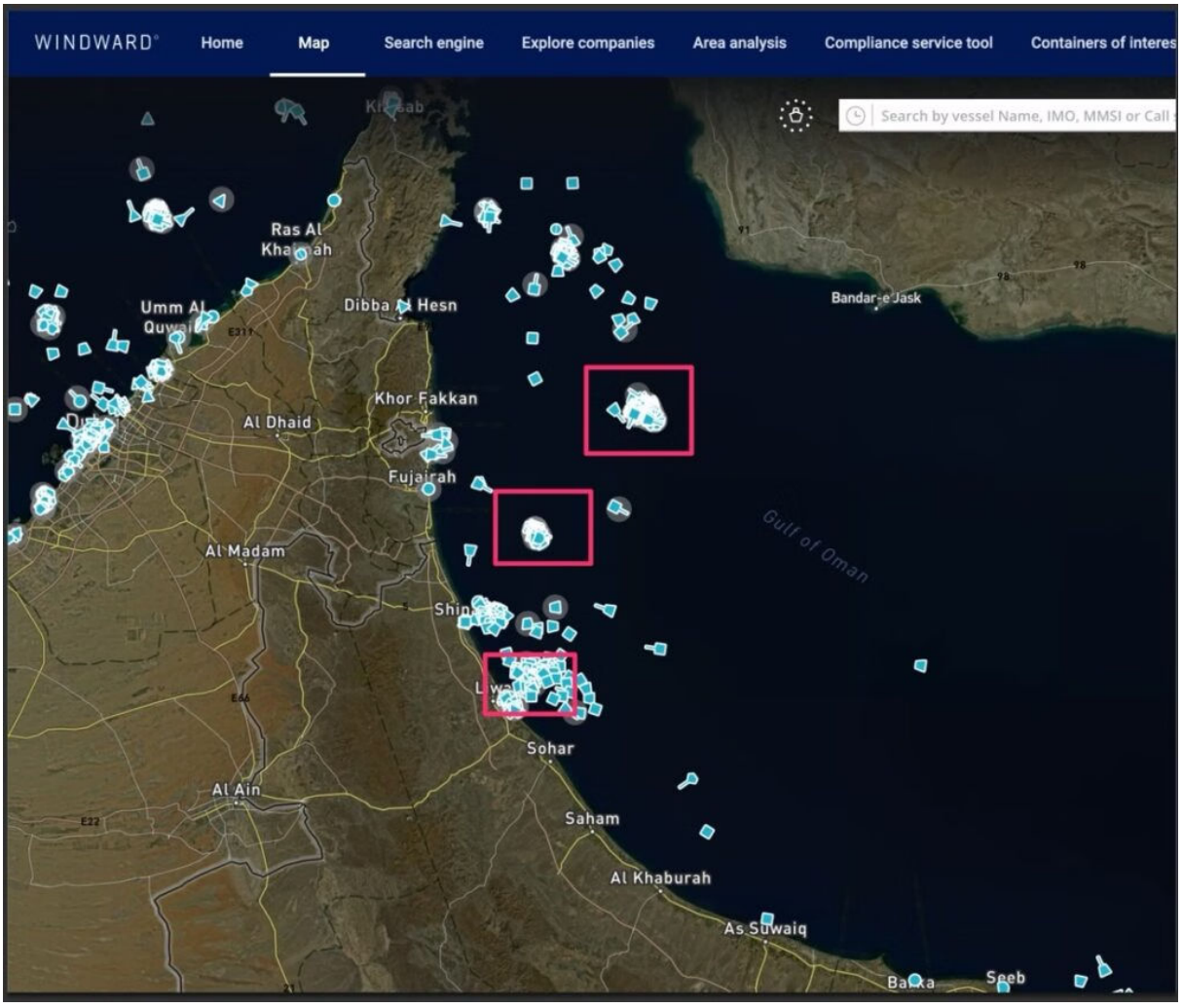
with historical patterns during IRGC operations: Iranian electronic warfare outposts on Abu Musa Island, located at the eastern entrance to the Strait, have been linked to GPS jamming incidents since at least 2019.

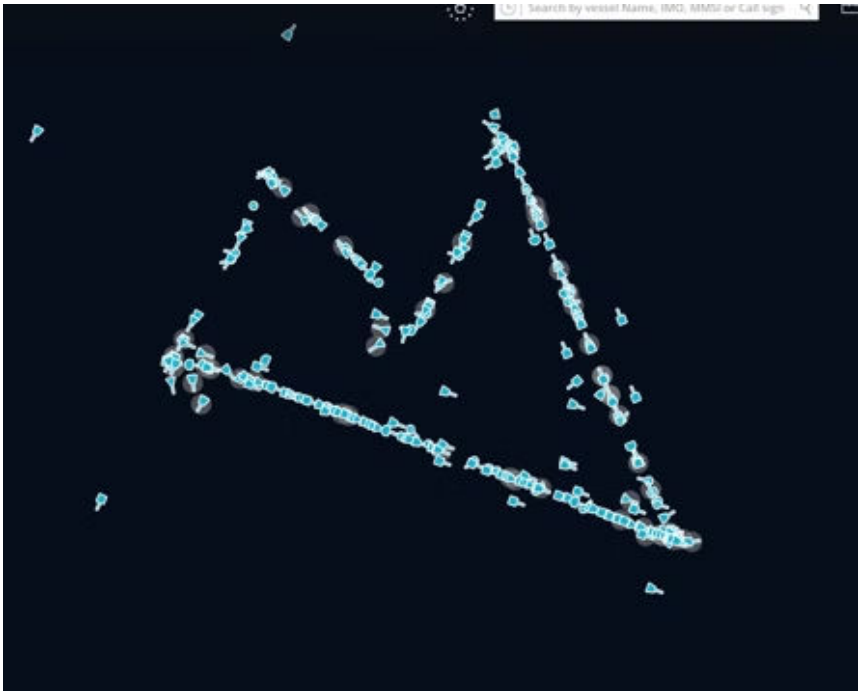
The practical consequence of the 2026 jamming campaign is distinct from historical precedent in both scale and target. Vessels are receiving false position data placing them at airports, inside nuclear power facilities, or miles inland — causing navigation computers to compute grossly incorrect positions while crews have no indication the system has failed. AIS signals have been diverted to the Barakah Nuclear Power Plant in the UAE, creating false positive sanctions risk and compliance breaches for banks, charterers, insurers, and other marine service providers who screen AIS data for Iranian port calls. A very large crude carrier waiting to load off Qatar had its AIS signal jammed to six different geographic positions within a single 24-hour period. The electronic warfare campaign has therefore generated compliance exposure for legitimate operators — triggering false positive sanctions alerts — while simultaneously providing a cover environment in which genuinely dark shadow fleet vessels can operate with reduced risk of detection.

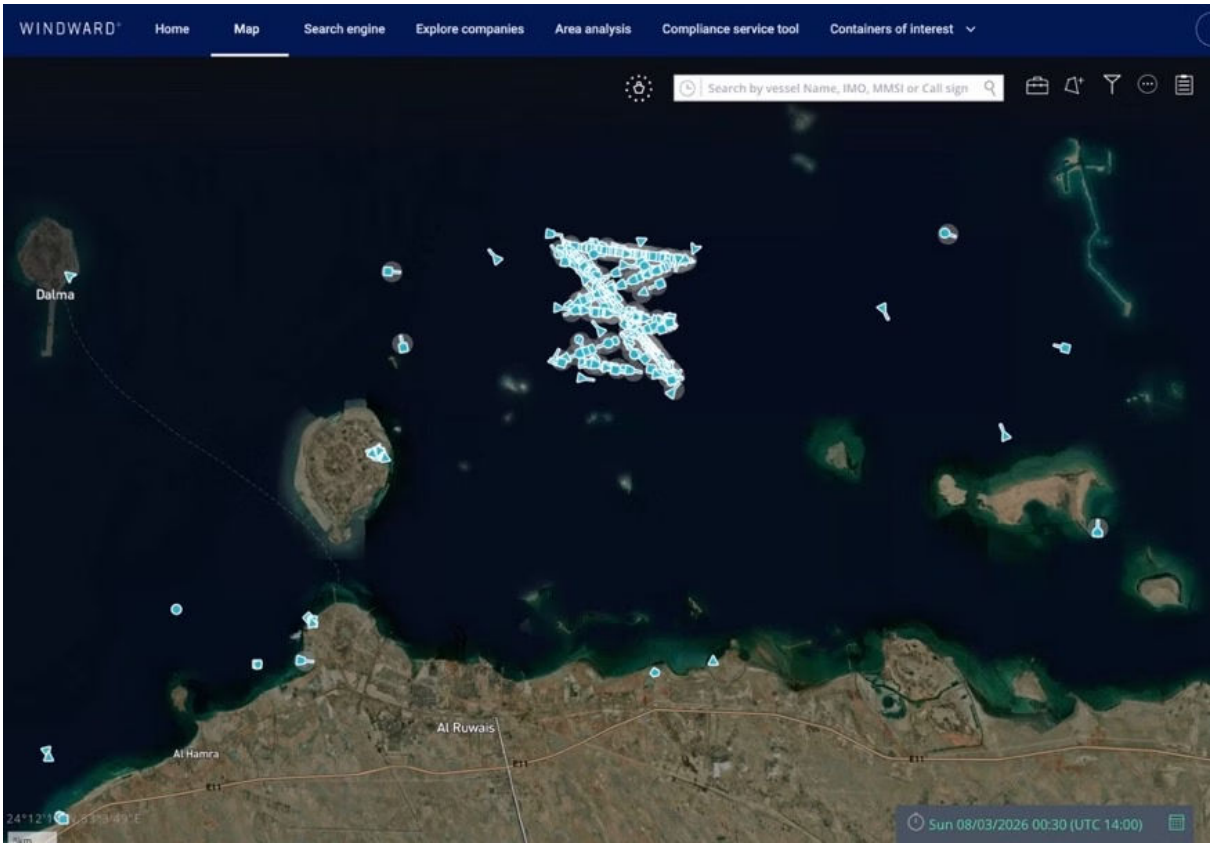
Dimitris Ampatzidis, senior risk and compliance analyst at Kpler, confirmed that the GPS interference affected approximately half the vessels in the Gulf and Gulf of Oman at peak disruption. Todd Humphreys, director of the University of Texas Radionavigation Laboratory, assessed that the disruptions in the Gulf carry hallmarks of deliberate state-level electronic warfare, noting that jamming overwhelms satellite signals while spoofing replaces legitimate signals with false ones — meaning receivers compute incorrect positions while crews believe systems remain functional.

Bloomberg correspondents aboard stranded tankers documented that when vessels attempted to transit out of the Gulf of Oman, GPS systems were subject to interference requiring crews to navigate using radar alone — a pre-electronic navigation capability that significantly reduces safe transit speed through one of the world's most congested shipping corridors.

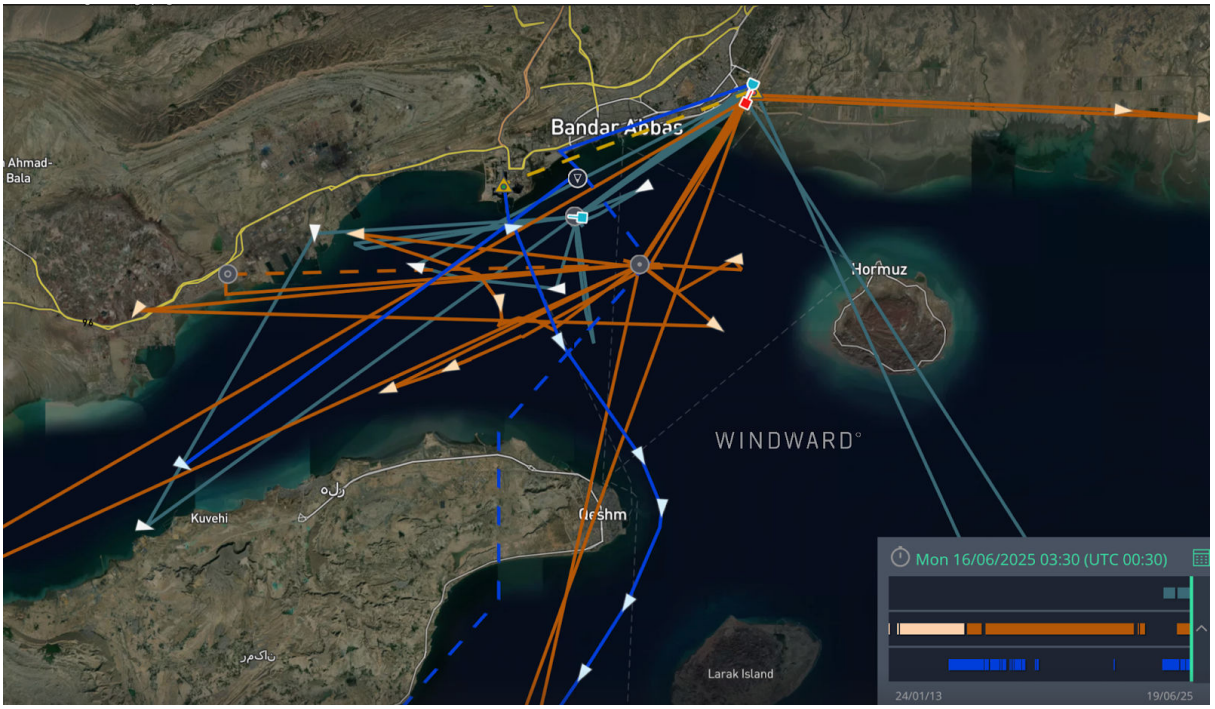
[GPS jamming disrupts more than 1,100 ships in the Middle East Gulf within 24 hours of Operation Epic Fury. AIS signals erroneously placed vessels at Al Hamra airport, over the Barakah Nuclear Power Plant, and on Iranian inland territory. At least 21 new jamming clusters identified]


WINDWARD
Home
Map
Search engine
Explore companies
Area analysis
Compliance service tool
Containers of interes
Search by vessel Name, IMO, MMSI or Call
Ras Al Khaimah
Umm Al Quwain
Dibba Al Hesn
Bandar-e Jask
Khor Fakkan
Al Dhaid
Fujairah
Gulf of Oman
Al Madam
Sohar
Al Ain
Saham
Al Khaburah
As Suwaiq
Saeb





[GPS jamming surge escalates — over 1,650 ships affected across the Gulf of Oman and Middle East Gulf, up 55% from the initial 1,100. Jamming patterns evolve from circular crop-circle formations into zig-zag straight lines spanning multiple geographic positions within single 24-hour windows, indicating deliberate signal engineering rather than passive interference]



[GPS jamming saw ships' AIS signals erroneously show them on land in Iran as they transited the Strait of Hormuz]

3.8 The Stryker Wiper Attack: Cyber as Wartime Financial Disruption

The most significant documented cyber event of the conflict's financial disruption campaign is the March 11, 2026 wiper attack against Stryker Corporation, a $22 billion Michigan-headquartered medical technology company operating in 79 countries. The attack was claimed by Handala Hack, an IRGC-linked advanced persistent threat group also designated as Void Manticore and Storm-842, which stated the operation was retaliation for a US-Israeli airstrike on an Iranian school on February 28, 2026.

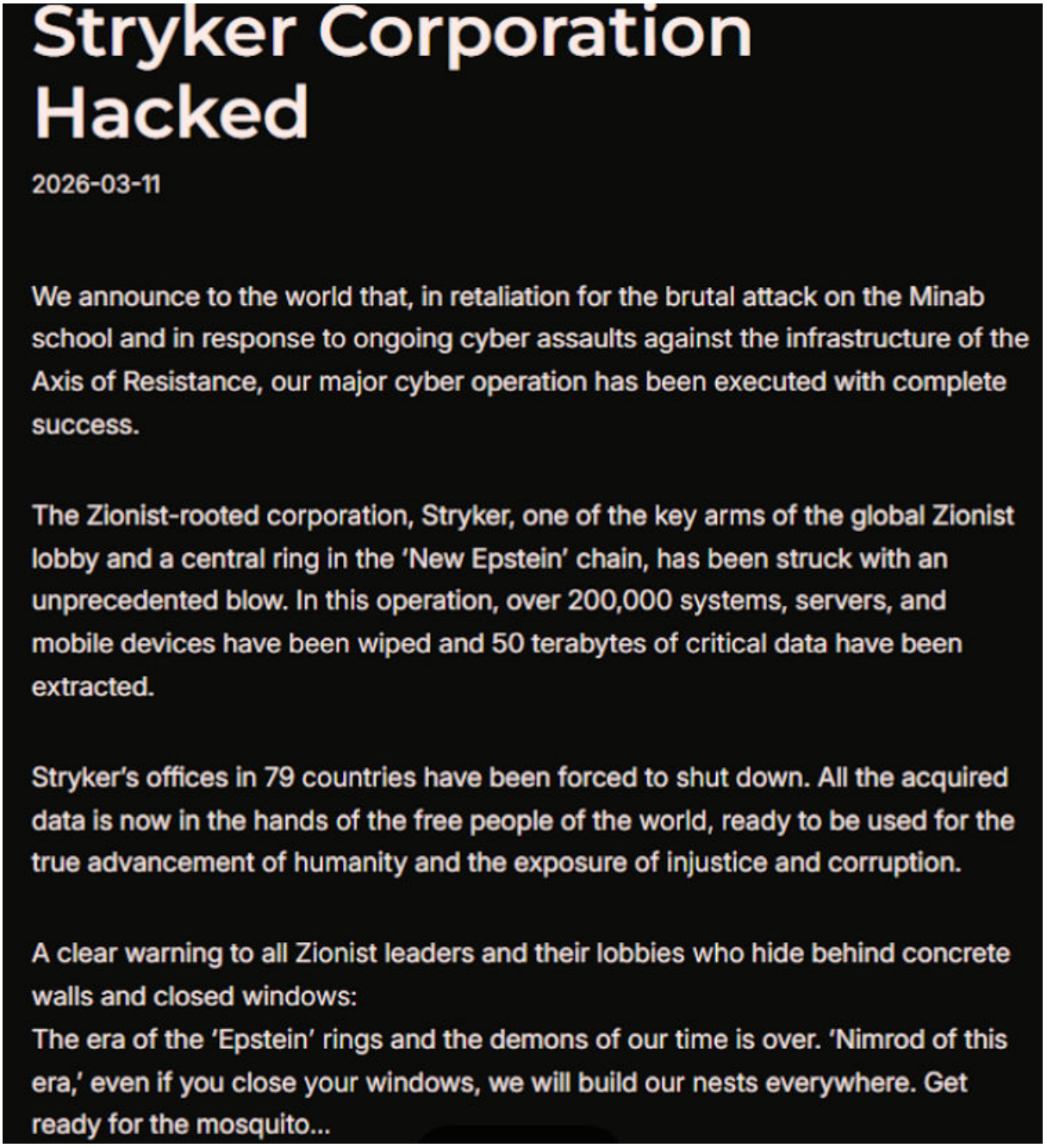
At 3:30 AM EST on March 11, Handala triggered simultaneous factory resets on over 200,000 Stryker corporate devices across 79 countries. The group did not deploy malware. Instead, it hijacked Stryker's own Microsoft Intune mobile device management platform and used it to push operating system reset commands across the company's entire enrolled device fleet — destroying data on servers, workstations, and mobile devices simultaneously with no possibility of recovery. Approximately 50 terabytes of sensitive corporate data were also exfiltrated, with threats of public release. In Maryland, paramedics lost the ability to transmit ECGs to hospitals, illustrating the medical supply chain disruption consequence of a cyberattack on a medical device manufacturer.

The Department of Justice formally attributed the attack to Iran's Ministry of

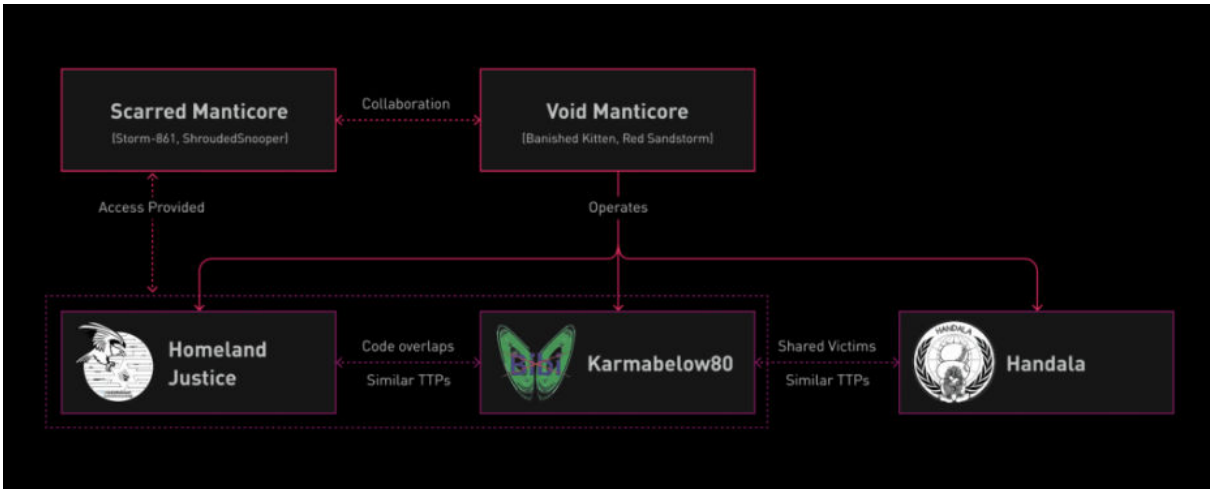
Intelligence and Security (MOIS) on March 21, 2026, and the FBI seized four Handala domains including Handala-Hack.to. Within hours, Handala launched replacement infrastructure and publicly mocked the seizure on Telegram. The State Department offered $10 million for information leading to the perpetrators. Research by security firm Push Security identified significant overlap between Handala (Void Manticore) and Scarred Manticore (APT34/OilRig), indicating coordination between MOIS and IRGC cyber assets. Both APT33 and Agrius — other Iranian IRGC-sponsored APT groups with documented histories of deploying destructive wiper malware against industrial, utility, and government targets — have now been confirmed as operating in the same broader attack ecosystem.

On the same day as the Stryker attack, the IRGC's Khatam al-Anbiya Headquarters issued a formal statement declaring US and Israeli-linked economic centres and banks as legitimate targets, warning civilians to remain at least one kilometer from such institutions. State-affiliated Iranian media simultaneously published a target list naming Google, Microsoft, and Nvidia, describing their regional infrastructure as Iran's new targets.

The financial disruption implications of the Stryker attack extend beyond the immediate operational damage. Stryker holds a $450 million US Department of Defense contract, making its supply chain disruption a national security event, not merely a commercial one. The use of a device management platform — rather than custom malware — as the attack vector means that any large organization using Microsoft Intune or similar enterprise device management systems, whose administrator-level credentials have been compromised via phishing or credential theft, faces structurally equivalent exposure. Security researchers at Censys identified nearly 2,000 Internet-facing hosts attributable to Stryker following the attack, with over 150 maintaining active login interfaces — confirming that even post-attack the organization's external attack surface remained substantially exposed.



[A manifesto posted by the Iran-backed hacktivist group Handala, claiming a mass data-wiping attack against medical technology maker Stryker]



[Operational interconnections of Void Manticore. Void Manticore is an Iranian threat actor affiliated with the ministry of intelligence and security. Known to conduct data destruction and espionage attacks]

SECTION 4: ECONOMIC QUANTIFICATION — THE FAIR RISK MODEL APPLIED

4.1 The Blockade Loss Event: One-Month Cost Framework

The Dallas Federal Reserve's model, published March 2026, establishes the primary quantification baseline. The removal of approximately 20 percent of global oil supply during Q2 2026 is expected to raise WTI to $98 per barrel and lower global real GDP growth by an annualised 2.9 percentage points in that quarter. If the Strait reopens after one quarter, the oil price drops but the level of real GDP remains 0.2 percent below its pre-closure baseline by year-end 2026. If disruption extends to two quarters, the year-end deficit rises to 0.3 percent. Three quarters of disruption produces a 1.3 percentage point reduction in full-year GDP growth — a near-recession scenario.

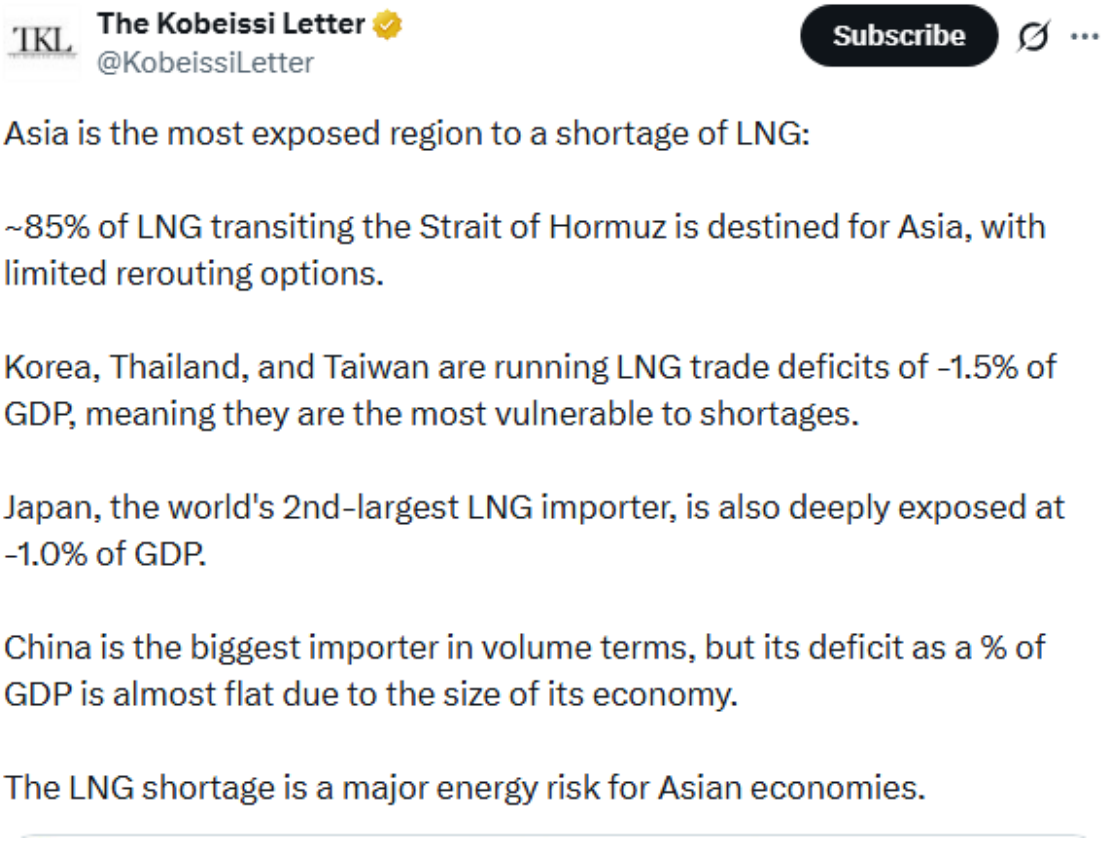
The IMF April 2026 World Economic Outlook applied its severe scenario to produce the most actionable number: global growth would be reduced by 1.3 percentage points, bringing the world to approximately 2 percent growth — the threshold historically associated with global recession, which has occurred only four times since 1980.

Brent crude was at $60.18 at end-2025. By 25 February 2026 it had risen to $71.40, a 19 percent increase. By April 2026, with the blockade active, futures dropped from $95.02 on optimism about ceasefire talks. For every $10 sustained increase in oil prices, academic modelling projects approximately 0.4

percentage points of GDP growth reduction and 1 full percentage point of inflation increase.

This binary framing from the world's largest asset manager is the most concise market sentiment signal available — it confirms that institutional capital at the highest level has already priced out any moderate scenario, treating the Hormuz situation as a discrete binary rather than a manageable gradient risk.

4.2 Country-Level GDP Impact: Japan, South Korea, and China



[These GDP-denominated LNG deficit figures are the single most actionable number for treasury hedging purposes — they translate directly into current account deterioration and currency depreciation pressure, with Korea, Thailand, and Taiwan representing the highest-exposure positions in any energy-driven FX hedging model]

Japan: Between 60 and 75 percent of Japan's crude oil imports transit the Strait of Hormuz. Japan holds approximately 470 million barrels in strategic reserves — roughly 254 days of domestic consumption, the largest buffer among the three target nations. However, Japan also depends on Qatar for LNG, which accounts for approximately 20 percent of its total energy supply. The IMF's adverse scenario — a larger and more slowly fading energy supply shock — projects GDP growth declining by almost 1 percentage point in 2026 relative to the reference scenario, with larger losses in fossil fuel-intensive and import-dependent economies. Japan is squarely in that category.

South Korea: Faces the sharpest structural exposure of the three. Between 60 and 75 percent of crude oil imports transit Hormuz. Strategic reserves stand at approximately 190 million barrels — roughly 60 days of domestic consumption, the most vulnerable buffer of the three economies. Additionally, South Korea imported 64.7 percent of its helium from Qatar in 2025. Samsung and SK Hynix,

which together account for 18 percent of global semiconductor production capacity, use helium to cool silicon wafers and create vacuum environments in lithography. Domestic chip makers currently hold approximately six months of helium supply. A protracted blockade beyond that window creates a direct existential threat to South Korean semiconductor output, with cascading effects across global electronics supply chains.

Maritime insurance premiums for the Persian Gulf rose 50 percent, with major providers issuing war risk cancellation notices effective March 5, 2026.

China: China is materially exposed but more resilient. Approximately 80 to 91 percent of Iran's crude exports go to China — approximately 1.38 million barrels per day in 2025. Around 40 percent of China's oil imports transit Hormuz. Kpler estimated China had stockpiled 1.3 billion barrels by March 2026, approximately 120 days of consumption. A Strait blockade is expected to reduce Chinese refined oil output by 50 to 70 percent — a more severe production impact than stockpile buffers suggest, because crude substitution does not immediately translate into equivalent refinery throughput. China's GDP growth forecast was revised to 4.4 percent in 2026, down 0.1 percentage points, the smallest revision among the three target economies.

Mitigated costs via alternative pipelines: The Saudi East-West Pipeline and the UAE Habshan-Fujairah Pipeline together can redirect no more than one-third of the disrupted oil volumes, and none of the LNG. Iran has repeatedly struck export facilities near Fujairah, creating operational uncertainty for this alternative route. The pipeline mitigation therefore reduces but does not eliminate the economic damage floor.

4.3 The Selective Blockade Protocol as a Legal Exploit

Iran has implemented a selective transit approach — allowing vessels from China, India, and Russia while restricting or threatening those linked to the US, Israel, and their alliance network. This "Selective Transit" protocol effectively creates a $1 million per-vessel premium for non-hostile vessels, enforced through the threat of strike rather than formal tariff. Iran's justification exploits its non-signatory status to UNCLOS while invoking UNCLOS provisions on stateless vessels when convenient — a legal arbitrage that China's Jing'an Technology characterised in January 2026 as "jurisprudential arbitrage" allowing the construction of "fact-based jurisdiction." The IMF has noted that Iran has sought to institutionalise Hormuz control through a formal toll system as a post-conflict negotiating demand.

[Iran Foreign Policy Analyst Hamidreza Gholamzadeh: Iran is negotiating end of Hormuz blockade by conditioning passage on Yuan-denominated oil settlement. Analyst estimate: $3 trillion annual cost to the US dollar system, with hyperinflation and recession risk]

This is the most financially significant single data point in the entire investigation for CFOs and treasury leaders. Iran is not simply blocking ships — it is using the blockade as leverage to structurally accelerate de-dollarisation of global energy trade. If Yuan-denominated passage becomes the negotiated settlement, every Asian energy importer that accepts that arrangement exits the dollar settlement system for a primary commodity. The $3 trillion annual figure cited represents the estimated reduction in dollar-denominated oil trade volume, directly compressing petrodollar recycling into US Treasuries, weakening the dollar's structural bid, and amplifying the inflationary feedback loop the IMF has already flagged. This is the financial off-ramp sabotage scenario described in the investigation mandate — not through cyberattack on price-cap infrastructure, but through a geopolitical protocol exploit that

achieves the same outcome: sustained market volatility and structural dollar erosion as Iran's primary war economy objective.

4.4 Third-Party Risk: JIT Industries with the Highest Blast Radius

Semiconductor manufacturing (South Korea, Taiwan): Dual exposure through both crude oil and helium, with six-month supply buffers already consuming in the current crisis.

Pharmaceutical cold chain and air freight: Dubai International Airport handled 95.2 million passengers in 2025. The suspension of operations there disrupts transit for 2 million annual passengers and severs the primary logistics link between Western and Asian markets. Extended routes across Central Asia or Africa increase pharmaceutical and electronics air-freight costs significantly, directly compressing JIT inventory windows.

Fertilizer and agriculture: Qatar and UAE LNG account for 99 percent of Pakistan's LNG imports, 72 percent of Bangladesh's, and 53 percent of India's. Natural gas feedstocks for fertilizer production are among the first casualties of LNG disruption. India's agriculture sector faces a dual physical and financial shock — supply disruption simultaneously with Brent-indexed LNG contract price escalation.

Automotive and heavy industry: Asia accounts for 45.7 percent of total crude imports that transit Hormuz. Most Asian economies are expected to reduce refined oil output by 30 percent under a sustained blockade, with Gulf nations at up to 90 percent reduction. This directly constrains just-in-time manufacturing in automotive, steel, and aluminium sectors that depend on continuous energy supply.

Sulfur supply chains: Qatar is a major sulfur exporter; disruption affects fertilizer manufacturing globally and has downstream effects on agriculture across the Middle East, South Asia, and Africa.

SECTION 5: THE WATER-TO-DOLLAR KILL SWITCH — DESALINATION AS AN ECONOMIC ECOCIDE VECTOR

5.1 Infrastructure Dependency as a Strategic Vulnerability

GCC countries account for approximately 60 percent of global water desalination capacity, operating more than 3,400 plants producing 22.67 million cubic metres of desalinated water per day. Qatar derives 99 percent of its drinking water from desalination. Bahrain exceeds 90 percent. Kuwait, Oman, Saudi Arabia, and the UAE derive 90, 86, 70, and 42 percent respectively. A 2008 US diplomatic cable from Riyadh, declassified in 2010, stated that the Jubail desalination plant supplied over 90 percent of Riyadh's drinking water and that the capital would have to evacuate within a week if the plant or its associated power infrastructure suffered serious damage.

5.2 Confirmed Attacks and Economic Cost

The conflict has already produced the first deliberate attacks on desalination infrastructure in the Gulf War since 1991. On 7 March 2026, an airstrike on a desalination plant on Qeshm Island disrupted water services for approximately 30 villages. On 8 March 2026, an Iranian drone attack caused material damage to a Bahraini desalination plant, injuring three persons. The Fujairah F1 power and water complex in the UAE sustained damage from falling debris from intercepted missiles, with subsequent uncertainty about the extent of desalination capacity impairment.

The Responsible Statecraft assessment confirms that targeting of desalination across the region has created a critical WASH crisis. Cities including Manama and Dubai rely almost entirely on desalination facilities. Attacks on Qeshm Island have already forced thousands to use unsafe water sources. In Doha and Jebel Ali, collateral damage to power supplies threatens to paralyse hospital hygiene and sewage systems. Qatar's Prime Minister assessed in an earlier scenario analysis that Qatar could exhaust potable water in as little as three days, prompting the pre-conflict construction of 15 large emergency water reservoirs.

Since most GCC desalination plants are physically integrated with co-generation power stations, attacks on electrical infrastructure also reduce water production. The direct per-day emergency cost attributable to desalination disruption has not been publicly quantified with precision, but the IMF April 2026 Regional Economic Outlook notes that GCC oil exporters directly affected by the war are now projected to contract GDP in 2026, with Qatar facing the steepest downward revision and the long-lasting adverse impact projected to leave output levels 2 percent below pre-war trends through 2030.

The attack footprint on GCC desalination infrastructure is substantially larger than the March 7–8 events documented in the original report. On March 30, 2026, Iranian forces struck a power and water desalination plant in Kuwait, killing one Indian worker and causing what Kuwait's Ministry of Electricity described as significant material damage to a service building. Iranian authorities denied responsibility and attributed the attack to Israel.

On April 3–5, 2026, Kuwait reported that Iranian drones damaged two power and water desalination plants and sparked fires at two oil facilities. The Kuwait Petroleum Corporation's Shuwaikh complex — housing both the oil ministry and KPC headquarters — was completely evacuated. Kuwait's Ministry of Electricity spokeswoman Fatima Abbas Johar Hayat confirmed the attacks caused serious material damage to the plants and the outage of two electricity-generating units.

The UAE defence ministry documented a separate wave of suspected Iranian missile and drone attacks on April 3, with at least 12 people injured in Abu Dhabi's Ajban area — predominantly Nepali and Indian workers — from debris from intercepted projectiles. The Fujairah F1 power and water complex sustained documented damage from intercepted missile debris, compounding the desalination capacity uncertainty flagged in the original report.

An npj Clean Water journal study published in 2026 documents approximately 5,000 desalination plants across the Middle East, producing 41.8 percent of global desalination capacity. Kuwait operates several major integrated power and desalination plants across its territory, including facilities at Shuaiba, Doha, Sabiya, and Al Zour — all of which together supply essentially all of Kuwait's potable water. Any disruption to these plants carries immediate household and industrial consequences given Kuwait's complete absence of natural freshwater reserves.

The Atlantic Council's Ginger Matchett, writing March 18, 2026, assessed that though Iran may not have deliberately targeted all of the plants affected in the first two weeks, the infrastructure is within short striking distance of Iranian launch platforms and could become a systematic target if the conflict escalates. The report specifically flagged that Kuwait and Bahrain's desalinated drinking water accounts for approximately 90 percent of supply — meaning any sustained attack on the installed plant base translates directly into a humanitarian crisis timeline measured in days, not weeks.

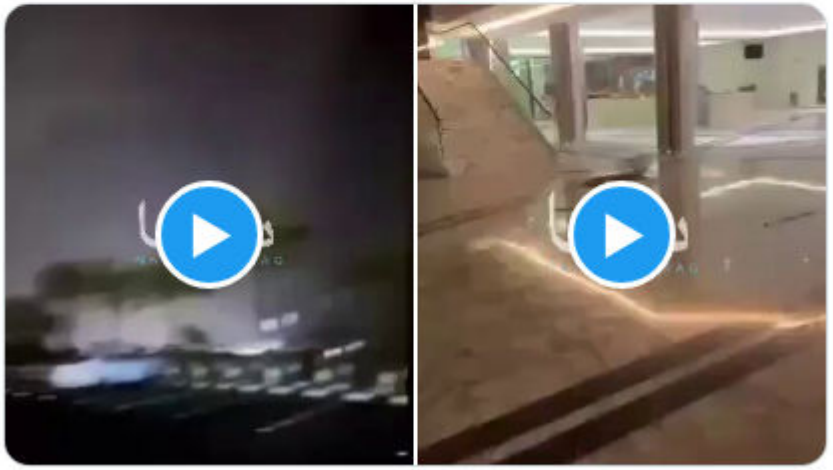
The economic quantification challenge for GCC desalination attack scenarios is compounded by the oil contamination pathway documented in Section 5.3. The acid rain plumes documented by Euronews in March 2026 — from refinery and

infrastructure fires carrying sulphur dioxide, nitrogen dioxide, PM2.5, heavy metals, and carcinogenic hydrocarbons — have already begun altering seawater chemistry in the Persian Gulf. If those contamination plumes reach the thermal desalination plant intakes concentrated along the UAE, Qatari, and Saudi coastlines, they would require complete facility shutdowns during the decontamination period — converting an air quality event into a water supply crisis without any additional military action.

THL **The Hormuz Letter**
@HormuzLetter · **Follow**

BREAKING: Kuwait's Ministry of Oil building has been hit in an Iranian attack.
Large fire reported at the ministry complex in Shuwaikh.

The ministry runs Kuwait's entire oil sector. Iran is now hitting the buildings that set Gulf oil policy, not just the facilities that produce Show more



4:44 AM · Apr 5, 2026

KUWAIT ARMY - الجيش الكويتي
@KuwaitArmyGHQ · **Follow**

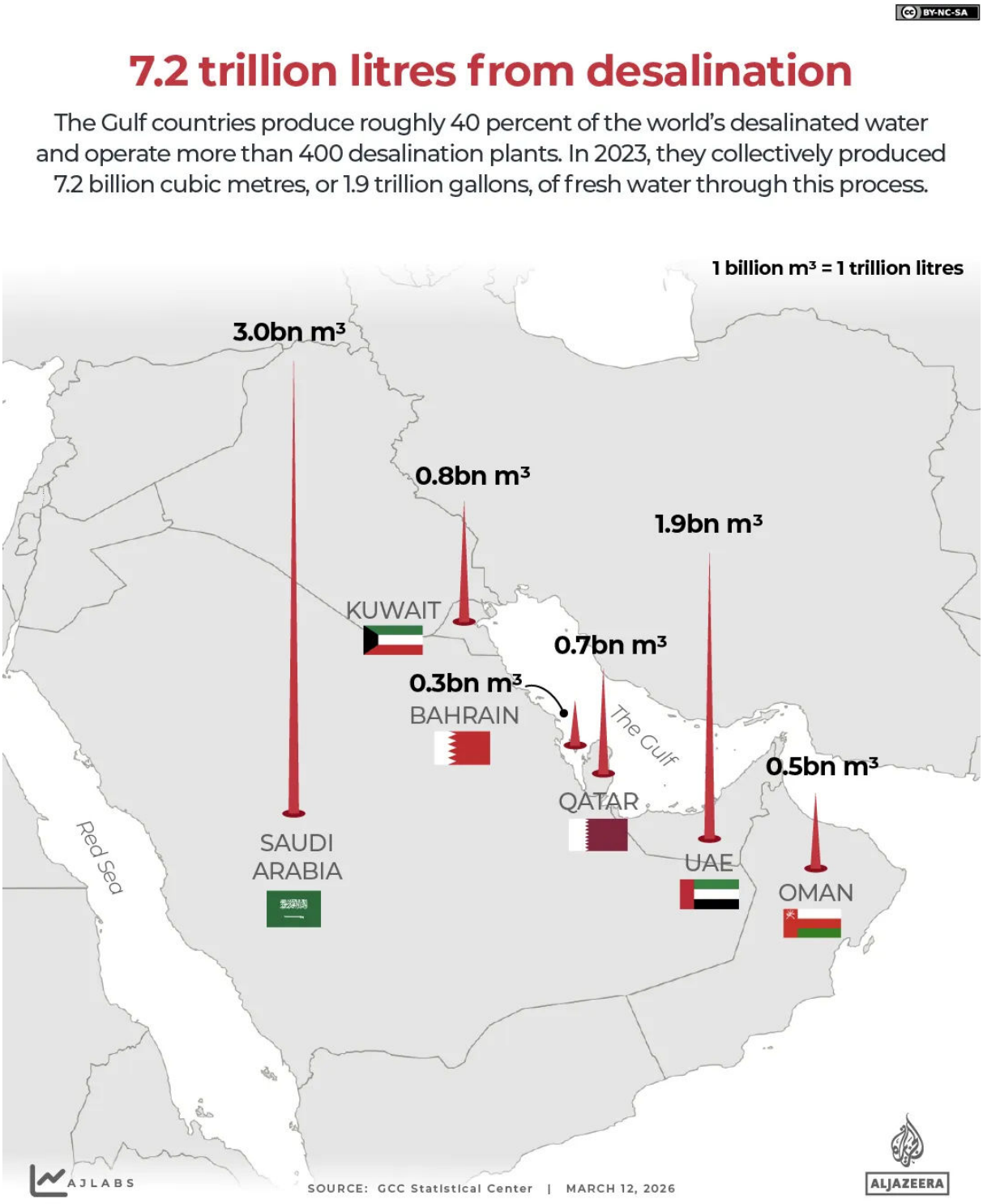
تتصدى حالياً الدفاعات الجوية الكويتية لهجمات صاروخية وطائرات مسيرة معادية.

تنوه رئاسة الأركان العامة للجيش أن أصوات الانفجارات إن سمعت فهي نتيجة اعتراض منظومات الدفاع الجوي للهجمات المعادية.

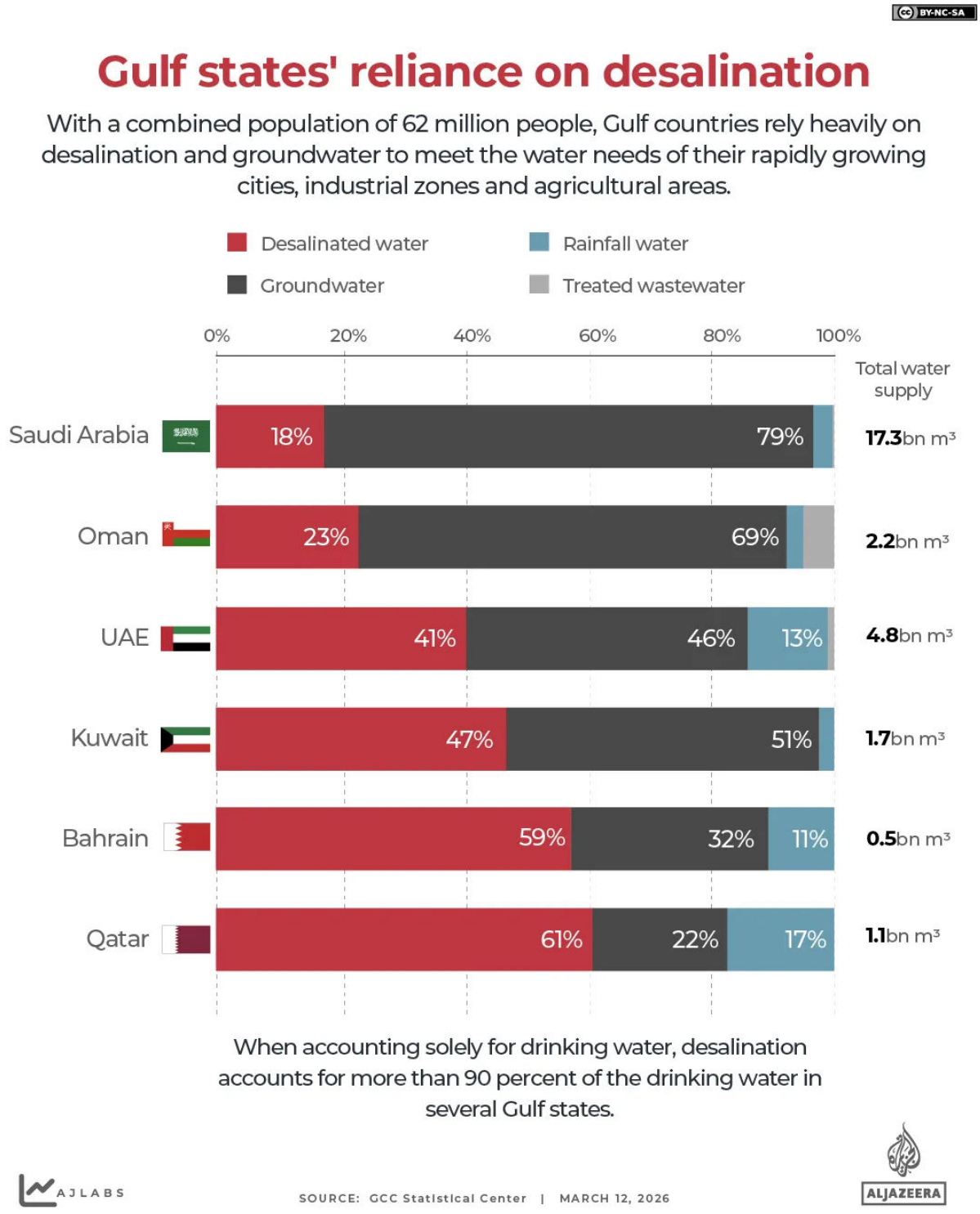
يرجى من الجميع التقيد بتعليمات الأمن والسلامة الصادرة عن الجهات المختصة. Show more

4:15 AM · Apr 5, 2026

[Smoke rises from an area of Kuwait's international airport after a reported drone strike on April 1, 2026]



[As the US-Israel war on Iran escalated, the region's dependence on desalination emerged as a critical vulnerability]



5.3 Oil Contamination as a Desalination Kill Vector

Research on Qatar's water security has specifically documented that oil spills and red tides can interrupt desalination operations or force complete facility shutdowns for extended periods. An oil infrastructure strike that contaminates Persian Gulf seawater intakes would not only destroy the source of drinking water for millions of people but would simultaneously destroy the industrial

water supply for Qatar and Bahrain's petrochemical and data centre sectors, which together consume more than 50 percent of those countries' desalinated water output. The acid rain plumes already documented by Euronews in March 2026 — containing sulphur dioxide, nitrogen dioxide, PM2.5, heavy metals, and carcinogenic hydrocarbons from refinery and infrastructure fires — represent the leading edge of this ecocide scenario.

The IMF April 2026 report explicitly recommends that GCC economies require sustained investment in the resilience of water, power, and digital networks, and that water infrastructure vulnerability represents a primary long-term fiscal risk for the region.

SECTION 6: THE IRGC FINANCIAL NETWORK IN LATIN AMERICA — WESTERN HEMISPHERE EXPOSURE

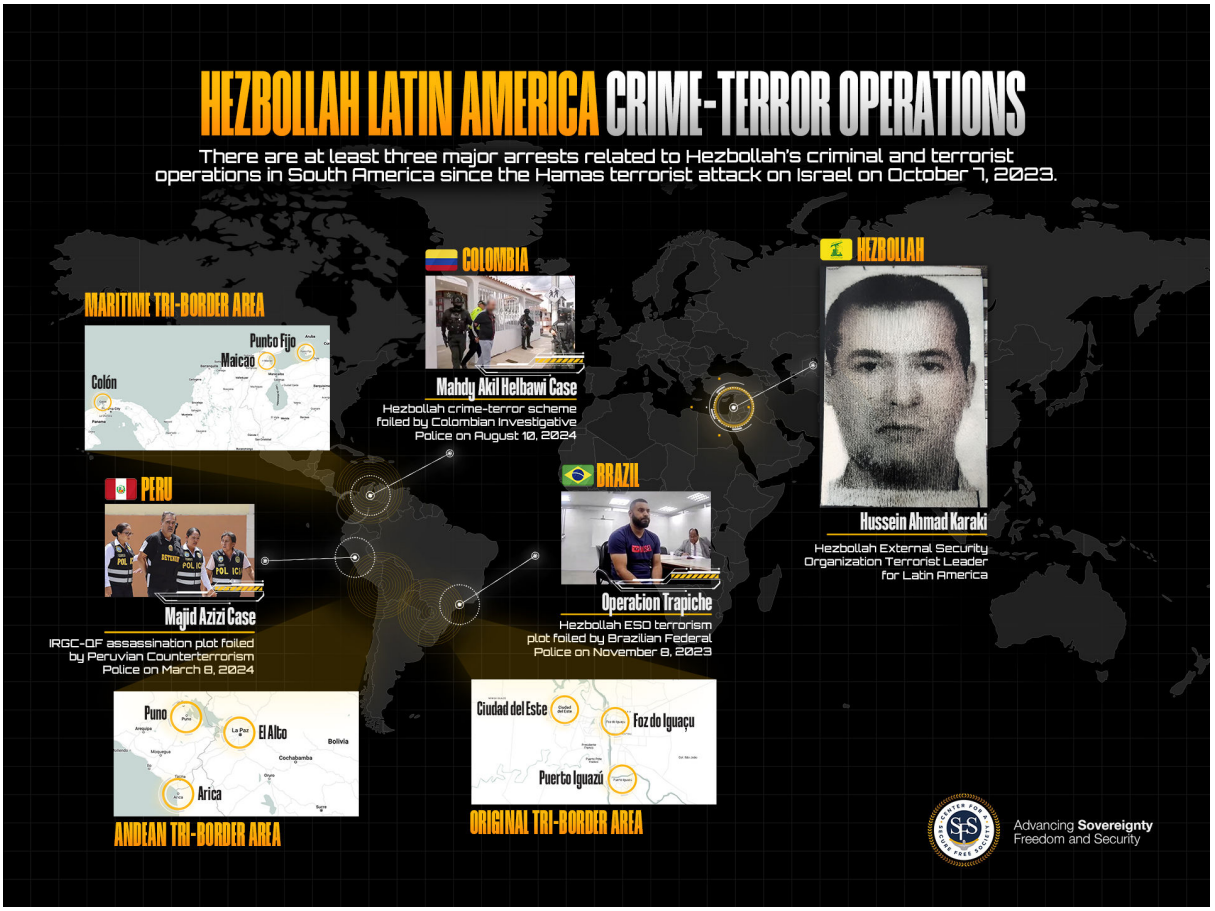
6.1 Network Architecture and Historical Depth

Iran's Quds Force has constructed a parallel financial and logistics infrastructure in Latin America over three decades that now functions across four distinct operational layers: Venezuela (where IRGC-linked personnel have colonized state institutions and senior officials have faced US federal indictment on narco-terrorism charges); the Tri-Border Area of Argentina, Brazil, and Paraguay (where Hezbollah's financial infrastructure has generated hundreds of millions of dollars over four decades through trade fraud, drug trafficking, and money laundering); Mexico (where the Quds Force has made documented contact with transnational criminal organizations, including at least one confirmed conspiracy to use cartel logistics for a targeted assassination on US soil); and Turkey (which serves as the primary geographic bridge between the Latin American network and the Iran-Hezbollah financial pipeline through Istanbul's exchange-house ecosystem).

The 2011 Arbabsiar plot, the 2024 Quds Force-directed assassination campaigns against US political figures, and the MI5-documented more than 20 Iranian-facilitated plots in the United Kingdom in 2025 collectively demonstrate that Tehran exercises this kinetic capability when the risk-reward calculation supports it. The financial infrastructure sustaining Iran's shadow fleet therefore functions simultaneously as a pre-positioned lethal capability in the Western Hemisphere — the same shell companies, exchange networks, and hawala brokers that convert oil revenue into operational funds also constitute the

logistical substrate from which assassination operations can be resourced and launched.

JINSA's cross-continental threat assessment, published November 2025, documents the bilateral relationship as built on mutual circumvention of Western sanctions through a combination of oil-for-gold exchanges, joint weapons manufacturing (including Iranian drones and loitering munitions produced on Venezuelan soil), defense pacts including a 20-year agreement signed in 2022, and the integration of Hezbollah-linked front companies for money laundering. Cartel de los Soles, the Venezuelan military narco-trafficking network, and Iran's IRGC-QF operate as structural partners in the shared logistical apparatus.


HEZBOLLAH LATIN AMERICA CRIME-TERROR OPERATIONS
There are at least three major arrests related to Hezbollah's criminal and terrorist operations in South America since the Hamas terrorist attack on Israel on October 7, 2023.
COLOMBIA
Mahdy Akil Helbawi Case
Hezbollah crime-terror scheme foiled by Colombian Investigative Police on August 10, 2024
HEZBOLLAH
Hussein Ahmad Karaki
Hezbollah External Security Organization Terrorist Leader for Latin America
MARITIME TRI-BORDER AREA
Punto Fijo
Maicao
Colón
PERU
Majid Azizi Case
IRGC-QF assassination plot foiled by Peruvian Counterterrorism Police on March 8, 2024
BRAZIL
Operation Trapiche
Hezbollah ESO terrorism plot foiled by Brazilian Federal Police on November 8, 2023
Puno
El Alto
La Paz
Bolivia
Cochabamba
Arica
ANDEAN TRI-BORDER AREA
Ciudad del Este
Foz do Iguaçu
Puerto Iguazú
ORIGINAL TRI-BORDER AREA
Advancing Sovereignty
Freedom and Security

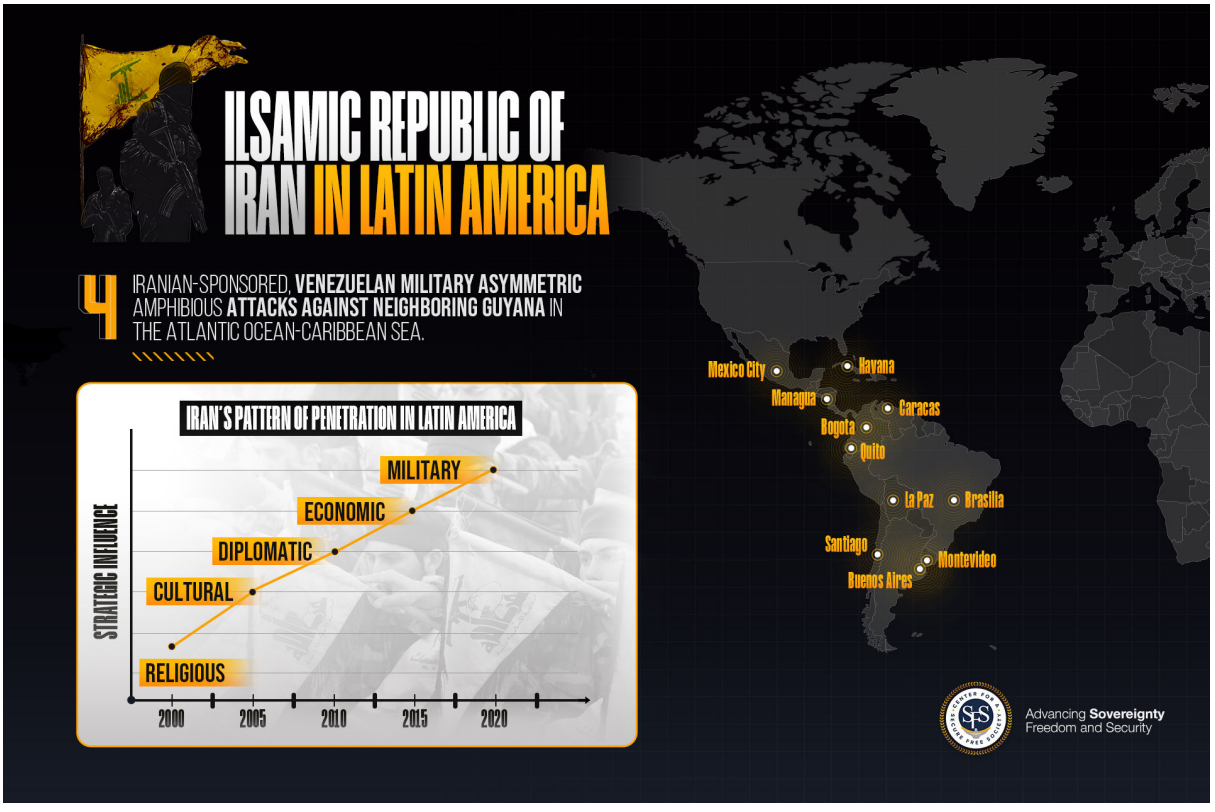

IRAN'S PROXY WARFARE COMING TO LATIN AMERICA
Hezbollah
Hamas
Houthi Rebels
Syria
Iraq
Iran
Yemen
IRANIAN DRONES ON DISPLAY IN VENEZUELA
March 09, 2022
BOLIVIAN DEFENSE MINISTER VISITS IRAN TO SIGN A NEW DEFENSE AGREEMENT
July 21, 2023
IRANIAN NAVAL WARSHIPS IN BRAZIL
February 27, 2023
EMTRASUR
IRGC-PILOTED VENEZUELAN CARGO PLANE DETAINED IN ARGENTINA
June 06, 2022
Advancing Sovereignty
Freedom and Security

[Iran's Foreign Minister Mohammad Javad Zarif and Jorge Arreaza shake hands and pose for a photo during the Ministerial Meeting of the Non-Aligned Movement Coordinating Bureau in Caracas, Venezuela. The dual-use nature of Iran's cooperation with the Maduro regime, layered with the illicit finance connections of its facilitators and Hezbollah's established crime-terror network in Venezuela requires a robust response from the international community. Picture taken July 20, 2019]

6.2 The Maduro Capture and Its Network Consequences

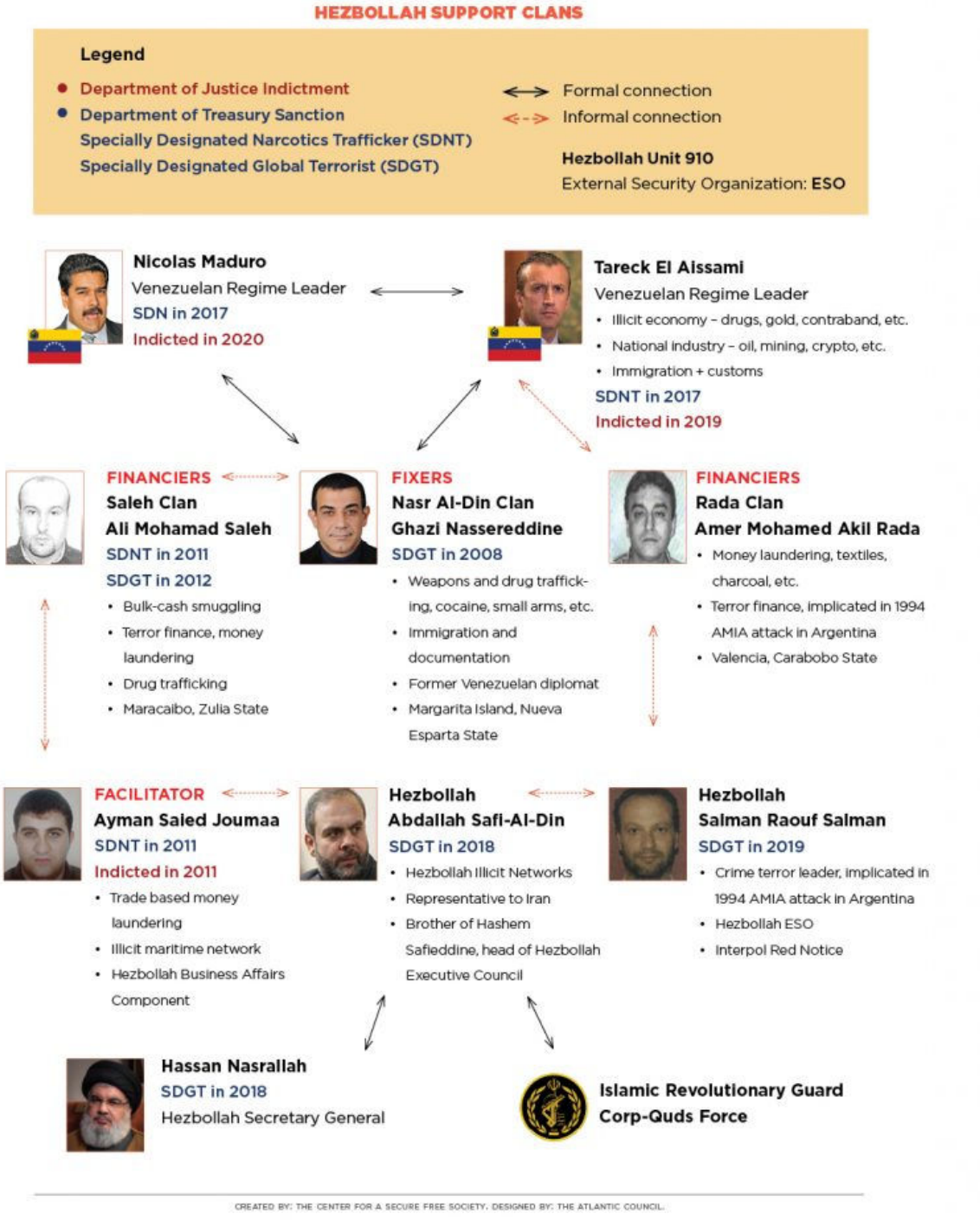
A significant structural disruption to the Latin American node of Iran's financial network occurred in January 2026 with the capture of Nicolas Maduro by US forces and the transfer of power in Caracas to Delcy Rodriguez. Venezuela had provided the primary logistical and diplomatic cover for IRGC-QF operations across South America. Without a reliable government umbrella in Venezuela, the same amounts of shadow financing become objectively harder to maintain, potentially forcing Tehran to restructure logistics toward more expensive routes — likely through Turkey, Oman, or Central African transit points that have historically served as secondary financial corridors.

The Viktor Artemov connection documented in the original report — a Ukrainian national with IRGC-QF links appearing in both the Iranian shadow fleet network and the Venezuela oil-for-gold operation — illustrates the personnel continuity of the network even as state sponsorship in Venezuela becomes more uncertain. Artemov represents the human infrastructure layer that persists across geographic restructuring events.



[For more than two decades, Venezuela functioned as a strategic hub for foreign regimes and militant networks far beyond Latin America. With the collapse of the Maduro system, a covert alliance spanning gold and drones came under unprecedented strain]

> **In Venezuela, Hezbollah's support network operates through compartmentalized, familial clan structures that embed into the Maduro regime-controlled illicit economy and the regime's political apparatus and bureaucracy.**



[Created by: The Center for a Secure Free Society. Designed by: The Atlantic Council]

6.3 The Muslim Brotherhood Pivot: Post-IRGC Proxy Finance

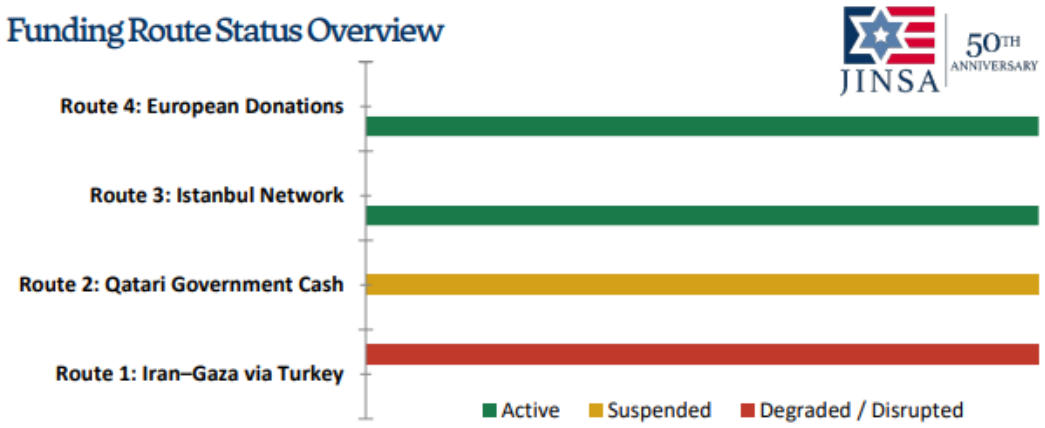
The JINSA March 2026 analysis documents a critical structural shift in Iran's proxy financing architecture triggered by the conflict: with the Central Bank of Iran's digital infrastructure incapacitated within the first 72 hours of Operation Epic Fury, and Iranian internet connectivity falling 99 percent from prewar levels, the traditional IRGC-mediated financial pipeline to Hamas and Hezbollah has been severely degraded. In response, the proxy network has pivoted to the Muslim Brotherhood's global financial apparatus as an alternative last-mile financing source, with operational anchoring increasingly in Doha and Istanbul/Ankara.

The Jabarin portfolio — Hamas finance director Zaher Jabarin's $500 million in Turkish real estate and stocks — is fully operational regardless of Hamas political leadership location. Many of the Doha-based NGOs feeding into the Istanbul network remain registered and active under Qatari law, notwithstanding Qatar's movement toward formal expulsion of Hamas leaders (accelerated after Hamas leadership's refusal to condemn Iranian strikes on Qatari soil in March 2026). As of March 2026, Qatar is heading toward a full political expulsion, but this does not affect the financial network's operational continuity.

The JINSA analysis identifies four parallel financing routes that converge on Gaza-based money changers converting inbound transfers into physical cash for Hamas commanders: an Iranian-Lebanese-Turkish money changer chain (Iranian funds move through Lebanon, then Turkish money changers, then into Gaza); a Qatari humanitarian NGO channel (charitable fundraising bundled into operational finance); a crypto rail using TRON/Tether wallets identified in the JINSA analysis as interacting with the same hawala networks used by the Zarringhalam shadow banking system; and direct transfers from Muslim Brotherhood branch structures in Europe and North America. Since January 2025, Iran has also sent more than $1 billion to Hezbollah through the exchange-house mechanism, establishing the operational precedent before that pipeline was degraded by the conflict.

For compliance teams, the JINSA analysis produces a specific screening implication: any financial institution whose counterparty universe includes Qatar-registered NGOs with stated humanitarian mandates, Turkish real estate holding companies with opaque beneficial ownership, or exchange houses with exposure to the hawala networks documented in the Zarringhalam profile (Section 1.3) should treat those relationships as potentially carrying Muslim Brotherhood-Hamas financial network exposure — regardless of whether those

counterparties appear on the SDN list, because the post-IRGC pivot is specifically designed to route through entities not yet designated.



Route 1 — Iran-to-Gaza (Degraded): Iranian funds were previously routed through Lebanon, then through money changers in Turkey, and finally into Gaza. By December 2025, Israeli and U.S. intelligence had confirmed that this network transferred hundreds of millions of dollars to Hamas leadership. Since January 2025 alone, Iran had transferred more than $1 billion to Hezbollah through this same exchange-house mechanism, corroborating the network's potential before it was crippled. The Iranian terminal of this route has been affected by the current conflict, but the Turkish exchange structure remains intact and is absorbing redirected funds formerly from other sources.

Route 2 — Direct Qatari Government Cash (Suspended for Now): Beginning in 2018, Qatar channeled $30 million a month to Gaza, deposited as physical cash. A joint United States-Israeli intelligence assessment in 2024 found that most of those funds had been used to support Hamas's military infrastructure, not civilian priorities. Internal Hamas documents seized by Israel make clear that the Qatari government directly funded Hamas military operations. This route has been suspended since October 2023, when the outbreak of conflict made physical cash delivery into Gaza impossible. Operation Epic Fury has foreclosed any near-term resumption.

Route 3 — Istanbul Network (Active Now — Main Route): This is the primary active channel. The charities in Qatar raise donations under humanitarian cover, then transfer money to Istanbul, where Zaher Jabarin, Hamas's director of finance (who was sanctioned by the U.S. Treasury in 2019) holds over $500 million worth of real estate and Turkish shares for Hamas. Funds then flow through currency exchange businesses into Gaza. U.S. Treasury records show that one exchange house alone sent more than $21 million to Hamas and its military wing from 2017 through 2019. In the last link in the chain, approximately ten money changers in Gaza — all known to Israeli intelligence — turn the funds into cash for Hamas field units.

Route 4 — European Donations (Active Now): Money gathered by charitable associations throughout Europe is channeled through Turkish exchange firms into Hamas' financial network. The Washington Institute has reported how Hamas uses MB-linked umbrella groups — including one that the U.S. Treasury established is still directly accountable to Hamas's military wing — as the backbone of this pipeline. U.S. Treasury analysis also determined that such transfers move through American banking systems, providing an opportunity for enforcement and exposure under U.S. law.

1. **Hamas as an Interoperability Layer:** Hamas acts as a vital bridge because it is the only group that has deep structural ties to both the IRGC and the global Muslim Brotherhood. Article 2 of the Hamas Covenant reads, "The Islamic Resistance Movement is one of the wings of the Muslim Brotherhood in Palestine." The U.S. Treasury's Office of Foreign Assets Control (OFAC) noted that Muhammad Ahmad Abd Al-Dayim Nasrallah, a Qatar-based Hamas operative, had close links to the Iranian regime and was responsible for providing tens of millions of dollars to Hamas, including the Qassam Brigade. This dual alignment enables Sunni MB resources to flow into a shared ecosystem that simultaneously sustains Shia-aligned IRGC purposes.
2. **The Shadow Banking Nexus:** On October 23, 2025, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) examined an estimated $9 billion shadow banking system that used front companies in the UAE and Turkey to move IRGC money through American correspondent accounts (accounts that U.S. banks maintain with foreign banks to process international transactions), before washing those funds through MB-controlled NGOs in Doha. In 2025, U.S. Treasury targeted networks of this nature on several occasions, such as its June 2025 targeting of the Zarginhalam brothers—Mansour, Nasser, and Fazlolah Zarginhalam are Iranian bankers and businessmen and key operators of a major "shadowing bank" network —that laundered billions for the IRGC-QF through both exchange houses and front companies.
3. **The Digital Backbone:** TRM Labs confirmed that Iranian state actors and MB-linked facilitators share clusters of TRON-based digital currency wallets and use high-risk exchanges such as Zedcex to move funds for Iran's proxy. Stablecoins— digital currencies pegged to the U.S. dollar to avoid price swings— accounted for 84% of the estimated $154 billion in illicit virtual asset transaction in 2025, with USDT (a fiat-backed stablecoin issued by Tether) on TRON being the most used instrument. The A7 wallet cluster — a $39 billion node that connects Russia and Iran — illustrates the scale of pre-positioned digital funds accessible to "Axis of Resistance" networks.

SECTION 7: ACTIONABLE INTELLIGENCE BY AUDIENCE

7.1 For CFOs and Global Treasury Leaders

The current crisis constitutes a sustained energy-driven inflation shock. The IMF models a global recession threshold breach under its severe scenario. Every $10 sustained increase in oil prices produces 0.4 percentage points of GDP reduction. With Brent having risen approximately 58 percent from end-2025 to peak blockade levels, the equivalent GDP toll is approximately 2.3 percentage points — already exceeding the Dallas Fed's one-quarter severe scenario. Currency hedging should account for depreciation pressure on import-dependent Asian currencies (South Korean won, Japanese yen, Indian rupee) against the USD. Energy derivatives positions should specifically price helium supply risk for semiconductor-exposed portfolios.

The primary red flag for financial institutions, per FinCEN's updated advisory, is transactions where a company's main receipts are from oil/commodity trading but its primary outgoing payments go to electronics companies in Hong Kong

or Chinese mainland. This is the Zarringhalam network signature and represents direct secondary sanctions exposure.

The structural de-dollarisation risk has moved from a theoretical scenario to a documented operational mechanism. Iran's crypto toll collection at Hormuz — denominated in Bitcoin, USDT, and yuan rather than dollars — represents the first instance of a sovereign actor successfully extracting regular, recurring dollar-equivalent revenue from global energy trade outside the dollar correspondent banking system, at scale, in real time. Each $2 million USDT payment from a laden VLCC to an IRGC-controlled wallet is a transaction that exits the petrodollar recycling chain permanently.

The $3 trillion annual estimate for dollar system impact, cited by analyst Hamidreza Gholamzadeh, represents the estimated reduction in dollar-denominated oil trade volume if yuan-denominated passage becomes normalized as the settlement mechanism. For CFO treasury modelling, the relevant scenario horizon is not the full $3 trillion figure but the subset of the $600 to $800 million in monthly toll revenue that never re-enters the dollar system at all, compounding at that run rate against a USD interest rate environment already absorbing an inflation shock from the oil price surge.

The secondary screening trigger for financial institutions, specifically for the Hormuz toll mechanism, is any transaction in which a shipping company or commodity trading house is making a USDT or Bitcoin payment to a counterparty wallet that cannot be verified as a legitimate maritime service provider, with a payment amount in the range of $1 to $3 million and a timeline consistent with a Gulf transit window. These transactions match the IRGC toll collection profile exactly and meet the FinCEN stablecoin risk criteria documented in Section 3.2.

7.2 For Maritime Insurance and Re-Insurance Underwriters

War risk premiums for the Persian Gulf have already risen 50 percent. Standard re-insurance coverage cancellations took effect March 5, 2026. The operational intelligence priority is vessel identity verification against both the OFAC SDN list and the Wikilran vessel tables, since a clean IMO number may now represent a stolen identity used by a sanctioned hull. The Wikilran dataset of 100-plus AFGS-linked vessels, including 20 actively sanctioned ones still operating and 13 non-designated vessels exposed as part of the IRGC supply chain, is the most granular vessel-level compliance resource currently available in open source.

The New Zealand P&I Club (Maritime Mutual Insurance Association) case — having provided insurance on vessels carrying $18.2 billion in Iranian oil and $16.7 billion in Russian energy products — establishes the reputational and regulatory exposure benchmark for underwriters who fail to screen against behavioral patterns rather than solely the SDN list.

The GPS and AIS jamming campaign creates a previously undocumented secondary compliance exposure for underwriters. AIS signals diverted by Iranian electronic warfare to Iranian territorial waters or ports — including Assaluyeh and other Iranian ports — are triggering false positive sanctions alerts in automated compliance screening systems. A vessel whose AIS transponder has been spoofed to display a position inside Iranian waters has, in the automated screening environment, apparently made an Iranian port call — which would trigger sanctions screening flags, policy review requirements, and potential denial of coverage renewal. Underwriters whose policy terms reference AIS-derived vessel position data should immediately review whether their policy language creates inadvertent coverage exposure from spoofed position data that cannot be distinguished from actual Iranian port calls without additional manual verification.

The WikiIran vessel identity theft programme creates a parallel exposure: a vessel owner may discover that their IMO number, flag documentation, Q88 records, and master's identity are actively in use by a sanctioned Iranian hull. This OFAC exposure exists without any knowledge of the violation by the legitimate vessel owner. For underwriters, the practical implication is that a clean IMO number with a clean AIS track and no SDN list flag may still represent a vessel whose identity has been stolen and is being simultaneously used to transport Iranian crude under the legitimate vessel's compliance cover. The WikiIran dataset of over 100 AFGS-linked vessels — including 20 actively sanctioned ones still operating and 13 non-designated vessels exposed as part of the IRGC supply chain — should be cross-referenced against every renewal in the Persian Gulf tanker book.

7.3 For Trade Compliance and GRC Teams

The shift from entity-based to behaviour-based designation means that a vessel not on the SDN list but displaying AIS spoofing, repeated STS activity in high-risk corridors, and shell-company management structures now carries presumptive sanctions risk. The FinCEN advisory's red flags should be embedded in counterparty due diligence as trigger criteria, not as post-hoc screening checks.

Specific immediate termination triggers based on this investigation:

Any relationship with Phoenix Ship Management FZE (UAE), Rukbat Marine Services Co (India), Golden Gate Ship Management (India), or Darya Shipping Private Limited (India), all designated December 2025.

Any business relationship touching Oriel Group, Corplinx Consultancy LLC FZ, House of Shipping Investment FZCO, Meritron DMCC, or Taylor Shipping FZCO, all designated April 2026.

Any vessel whose master appears simultaneously in two different vessel management systems — the WikiIran identity theft cases show this is a detectable signal.

Any counterparty in the UAE free zones whose ownership is non-transparent, whose trading partners are primarily in Singapore and Hong Kong, and which has multiple bank accounts across UAE financial institutions — this is the FinCEN-documented Zarringhalam network signature.

7.4 For Port Authorities and State Regulators

The Alang Beach ship-breaking mechanism (Section 2.4) presents a specific regulatory gap. Ship-recycling yards in India, Bangladesh, and Pakistan that process vessels with histories of AIS anomalies, flag changes, or opaque ownership are at the terminal end of the shadow fleet's full financial lifecycle. Port authorities in receiving jurisdictions at Chittagong and Gadani face the same exposure as Alang: vessels arriving with disabled AIS systems, multiple recent flag changes, and Marshall Islands or Panama single-purpose company ownership should be presumed to be shadow fleet assets in end-of-life cash-out mode until proven otherwise.

State regulators in India face a specific dual-exposure problem that has no clean resolution within existing regulatory frameworks: India imports more than 60 percent of its oil from the Middle East, making aggressive enforcement of shadow fleet access restrictions economically damaging, while simultaneously being the jurisdiction where OFAC-sanctioned vessels are being scrapped for hard currency. The February 2026 seizure of three Iranian oil tankers sanctioned by the US demonstrates growing bilateral enforcement cooperation — but the coexistence of active interdiction with active ship-recycling of sanctioned hulls within the same jurisdiction is the operational contradiction that no single regulatory response can fully address.