# Prana Hacktivist Network Exposes Iran's Sanctions Evasion Scheme

*By Catherine Perez-Shakdam - Executive Director Forum for Foreign Relations*

# Foreword

In an era of accelerating hybrid threats and state-enabled subterfuge, the revelations contained in this report illuminate a critical front in the contest between rules-based international order and malign actors exploiting its blind spots. The data leaks attributed to the Prana hacktivist network provide the most comprehensive insider's view to date of the apparatus sustaining the Islamic Republic of Iran's sanctions evasion economy.

This dossier should serve as both a wake-up call and a tool for the United Kingdom and its allies. The findings present a detailed anatomy of how Iran's military leadership—under the Armed Forces General Staff and the IRGC—has systematically exported sanctioned oil, laundered proceeds through intricate financial and shipping networks, and reinvested the gains into destabilising regional activities. The use of shell companies, spoofed shipping signals, falsified documentation, cryptocurrency, and even bullion to mask origin and ownership underscores the adaptive sophistication of Tehran's illicit architecture.

For British policymakers, intelligence professionals, and financial regulators, the implications are clear. The United Kingdom—through the Office of Financial Sanctions Implementation (OFSI), the National Crime Agency (NCA), and its global diplomatic network—has both the mandate and the means to confront this challenge. The report's UK-specific recommendations point to immediate and actionable paths: expanding designations under domestic sanctions law, reinforcing maritime domain awareness, tightening financial oversight through Companies House and FCA mechanisms, and applying sustained diplomatic pressure on jurisdictions and entities enabling Iran's network.

Equally, this case highlights the strategic utility of unconventional data sources. While Prana's methods fall outside formal intelligence channels, the group's disclosures have produced verifiable and operationally relevant insights, as reflected by corresponding actions from the U.S. Treasury and EU partners. In this context, governments must develop secure and ethical frameworks to analyse and act on non-state intelligence, particularly when such disclosures serve to expose violations of international law.

This report is not just a documentation of malfeasance—it is a call to disrupt the economic arteries fuelling Iran's missile development, nuclear ambitions, and proxy violence. It offers the UK Government and its allies a unique intelligence advantage. The test now lies in translating this transparency into coordinated action that closes loopholes, deters future evasion, and signals that Britain will not be a soft flank in the enforcement of international sanctions.

Let the facts revealed within stand as both an indictment and an impetus. As the Prana Network declares, "the corrupt should fear us as the truth empowers the oppressed."

*Catherine Perez-Shakdam - Executive Director Forum for Foreign Relations*

# Introduction and Background

A new and highly consequential hack-and-leak operation by the Prana Network, a cyber-activist collective affiliated with the broader *Anonymous* movement, has exposed the architecture of Iran's global sanctions-evasion apparatus. In a series of coordinated cyber intrusions over late 2023 and early 2024, Prana breached the internal servers of several regime-linked Iranian corporations—most notably Sepehr Energy Jahan (SEJ)[1]—and extracted thousands of internal documents, contracts, and email correspondences. These materials, verified in part by journalists at *Reuters* and analysts at *IranCyberNews.org*, offer unprecedented insight into how Iran continues to export sanctioned crude oil, bypass international financial controls, and fund its regional military ambitions in defiance of U.S. and EU sanctions.

At the centre of this network is SEJ, a nominally private energy company revealed to be a front for the Armed Forces General Staff (AFGS), Iran's top military command structure. SEJ is headed by Majid Azami, a senior oil broker with close ties to Ayatollah Khamenei, who has been sanctioned by the U.S. Treasury under Executive Order 13224 for material support to terrorism. According to internal communications and financial spreadsheets leaked by Prana, SEJ facilitated the illicit sale of over 65 million barrels of crude oil in 2023 alone, generating upwards of $4.2 billion in revenue—much of which was channelled into Iran's ballistic missile programme, nuclear development, drone production, and foreign proxy militias including Hamas, Hezbollah, and the Houthis.[2]

Beyond the borders of Iran, the leaked data also points to Qatar's alleged complicity in facilitating Tehran's operations. Documents and intercepted emails detail a secret series of meetings in Doha, where Azami and senior Iranian officials are reported to have negotiated access to $1.6 billion in frozen Iranian assets held in European financial institutions.[3] These efforts allegedly involved covert financial transfers using cryptocurrency and gold, and—critically—relied on personal relationships and alleged bribes to Qatari elites to ensure political and financial cooperation. Though Qatar has not officially responded to these allegations, the data implicates Qatari-based intermediaries in assisting Iran with the logistics required to evade Western monitoring systems.

---

[1] Iran Cyber News. "Sepehr Energy Jahan Company Hacked: Iran's Military Oil Front Exposed." *IranCyberNews.org*, April 24, 2024. https://irancybernews.org/sepehr-energy-jahan-company-hacked/#:~:text=It%20is%20worth%20noting%20that,io%20website.

[2] Parisa Hafezi and Mari Saito. "Special Report: How Iran Uses a Secret Network of Ships to Smuggle Sanctioned Oil." *Reuters*, March 13, 2024. https://www.reuters.com/graphics/IRAN-OIL/zjpqngedmvx/.

[3] Iran–Qatar Relations," Wikipedia, last modified April 2025, https://en.wikipedia.org/wiki/Iran%E2%80%93Qatar_relations.Anadolu Ajansı+2Wikipedia+2Eurasia Review+2

This report consolidates Prana's cyber-leaks into a coherent assessment of Iran's evolving sanctions-evasion strategy. It provides forensic documentation of smuggling practices—including tanker obfuscation, falsified cargo certificates, and shell company laundering—alongside a geopolitical analysis of state complicity and the failures of international enforcement. It concludes with a series of targeted recommendations for Western intelligence agencies, financial regulators, and maritime enforcement bodies, aimed at dismantling the SEJ network, tightening oversight on dual-use logistics, and countering the hybrid warfare strategies employed by Tehran in cooperation with regional allies.

# Prana Network Hacktivists and Their Operations

Prana Network emerged in late 2023 as a consortium of hacktivists targeting Iranian regime assets. In February 2024, Prana announced a major breach of an IRGC-linked shipping firm, Sahara Thunder, exposing daily operations of Iran's "ghost fleet" of oil tankers.[4] Then in April 2025, hackers affiliated with Prana (under the Anonymous banner) penetrated Sepehr Energy Jahan – a U.S.-sanctioned Iranian energy company – extracting roughly 6 GB of internal data. Prana's methodology involves infiltrating email servers and databases, then releasing troves of emails, contracts, and even blueprints on a public leak site (simorgh.io) for analysts to scrutinize. The group's stated motive is to "lift the lid" on Tehran's sanction circumvention and reveal secrets "the regime [tries] to hide". Independent investigators and reputable media (Reuters, Der Spiegel, etc.) have vetted portions of Prana's leaks, lending credence to their authenticity. Indeed, some leaks have quickly translated into real-world consequences – for example, the U.S.Treasury sanctioned Sahara Thunder as an Iranian government front just weeks after Prana's disclosure.[5] Prana's hack-and-leak operations thus represent a potent new source of intelligence on Iran's illicit activities, albeit one that requires careful validation.

## Unmasking Iran's Sanctions Evasion Network

The hacked data troves illuminate a sophisticated network by which Iran's military establishment secretly profits from oil exports despite Western sanctions. Sepehr Energy Jahan (SEJ) stands out as a linchpin of this network. Corporate records and leaked emails show SEJ was created as a front company under the Armed Forces General Staff (AFGS)to handle sanctioned oil deals. In fact, U.S. officials explicitly note that *"Sepehr Energy oversees [oil sales] on behalf of the AFGS,"* acting as the commercial arm of Iran's military. Majid A'zami (a.k.a. Majid Azami) – SEJ's managing director and an Iranian Oil Ministry official – was blacklisted by OFAC in November 2023

---

[4] "IRGC Front Company Sahara Thunder Hacked by PRANA Network," *Iran Cyber News Agency*, February 4, 2024, https://irancybernews.org/irgc-front-company-sahara-thunder-hacked-by-prana-network/

[5] "Treasury Targets Networks Facilitating Illicit Trade and UAV Transfers on Behalf of Iranian Military," U.S. Department of the Treasury, February 23, 2024, https://home.treasury.gov/news/press-releases/jy2295

for his role in this scheme. Another operative, Elyas Niroumand Toumaj, has been identified as coordinating oil shipments for SEJ and was sanctioned alongside Azami. These individuals oversaw a web of shell companies registered inside and outside Iran to disguise the true seller and end-use of Iranian crude. Notably, Prana's leak of SEJ's internal files revealed that multiple affiliate firms – *Sepehr Energy Paya Gostar Jahan* and *Sepehr Energy Hamta Pars*, among others – were incorporated in 2023 at the same Tehran address, stacking a corporate paper trail across different floors of an office building. This network of interlocking shell companies was deliberately created to obfuscate the AFGS's hand in oil transactions.[6]

Leaked correspondence underscores the direct involvement of Iran's military leadership in sanction-evasion deals. In draft contracts found in SEJ's email archives, the companies explicitly refer to themselves as acting on behalf of the "General Staff of the Armed Forces". One negotiation in 2023 with the state-run Persian Gulf Star Oil Company (a major refinery) described SEJ's affiliate as the *"deputy of the Armed Forces General Staff,"*clarifying that the ultimate guarantor of the deal was the Iranian military itself. Similarly, draft agreements for oil tanker charters show that the AFGS formally guaranteed all obligations of SEJ's front companies, effectively using the military's credit to reassure counterparties. These documents flatly contradict claims by SEJ executives that they had "no connection to the IRGC or armed forces." (Prana found that Azami and Niroumand, shortly after being sanctioned, wrote to the U.S. Treasury in December 2023 protesting that their company was purely in construction/trade and was mistakenly sanctioned due to name similarity. The internal evidence proves otherwise.) In sum, the leaks conclusively demonstrate that Iran's military – via the AFGS and IRGC – established and operated SEJ and its affiliates as a covert apparatus to sell oil outside official channels. Billions of dollars in proceeds have been generated through this network, money that should be easing Iran's economic woes but is instead diverted to military projects and proxy wars.[7]

## Oil Smuggling Tactics and Evidence of Evasion

Prana's first major leak – over 10,000 emails from the Sahara Thunder shipping company – provided a granular look at how Iranian oil is physically smuggled and laundered on the high seas. Sahara Thunder, ostensibly a private import-export firm, was unmasked as an IRGC-linked operator running a fleet of tankers carrying sanctioned Iranian crude.[8] The leaked emails included both forged and authentic bills of lading, internal GPS location updates, and crew instructions – all documenting a playbook of deception. For example, captains were ordered to change their ship's name and repaint identification markings mid-voyage to assume new identities once loaded with Iranian oil. Communications emphasized *"not to use any Iranian name/point/word"*

---

[6] "Sepehr Energy Jahan," *Wikipedia*, last modified May 13, 2025, https://en.wikipedia.org/wiki/Sepehr_Energy_Jahan.
[7] "Treasury Targets Oil Network Generating Hundreds of Millions of Dollars for Iran's Military," U.S. Department of the Treasury, February 8, 2025, https://home.treasury.gov/news/press-releases/jy2295.
[8] "How Iran Moves Sanctioned Oil Around the World," *Reuters*, January 7, 2025, https://www.reuters.com/graphics/IRAN-OIL/zjpqngedmvx/.

and to obtain *"Non-Iranian certificate(s)"* for cargoes. Bills of lading were falsified to show benign origins (e.g. Iraqi or Malaysian ports) in place of Iranian load terminals.

One illustrative case from the leaks involved the oil tanker *Remy*. Official documents claimed the Panama-flagged *Remy* loaded one million barrels of crude at Basra, Iraq and sailed for Malaysia in February 2023. In reality, the ship – temporarily renamed "Deep Ocean" – had taken on Iranian crude via a ship-to-ship transfer in the Persian Gulf. En route, the Remy transmitted fake AIS (automatic identification system) signals, "spoofing" its reported location to mask rendezvous points. Upon reaching the vicinity of China,[9] the cargo was split and transferred at sea to two other vessels, one of which pretended to be anchored far from the actual transfer site. Ultimately those tankers delivered the oil to port in Shandong, China – its Iranian origin successfully concealed through a multilayered ruse. This is just one example among dozens: the leaked Sahara Thunder files detail smuggling operations involving *34 ships* over 2022–2024, utilizing at least *92 shell companies* as registered owners or operators. Many of these vessels form part of Iran's sanctioned "ghost fleet," yet some (like the *Remy*, now renamed *Wilma II*) remained unsanctioned and active at the time of the leak. The scale of the evasion is enormous – Iran's petroleum exports topped $50+ billion annually in 2022-2023 despite sanctions, mostly via clandestine deliveries to China. The Prana leaks "open a window" into this shadow oil trade, offering hard evidence of how Tehran sustains high export volumes through document fraud, ship identity theft, and covert logistics.

*Large crude carriers loading at Iran's Kharg Island oil terminal. Prana's leaked emails reveal that Iranian tankers routinely engage in ship-to-ship transfers, false renaming, and forged documentation to hide the origin of oil exports.*

Beyond documents, Prana's haul included incriminating visual evidence. Hackers published photographs of signed contracts and correspondence from SEJ's files, highlighting clauses that tie the company to the military. One leaked email (screen-capped and shared by the hackers) showed SEJ insiders discussing strategies to dodge U.S. sanctions just days after the network was hit with sanctions in late 2023. These images were presented by Prana as proof of the regime's intent to deceive international authorities. The sheer volume and detail of the leaked data – bills of lading, charter party agreements, corporate registries, and internal memos – give investigators a rich dataset to map Iran's illicit oil supply chain end-to-end. Intelligence agencies are reportedly combing through the 6 GB SEJ archive now posted online to trace where the oil went and who facilitated its journey. Early analysis shows major buyers in China, India, Malaysia, and the UAE were fed by this network, often via middlemen companies in the Persian Gulf and South Asia. Some European firms also knowingly participated in these deals despite recognizing SEJ's state ties, according to Iran-based correspondence cited in the leak. The data thus not only documents Iran's tactics but also identifies a host of foreign enablers – shipping firms, brokers, and end purchasers – that form the backbone of the evasion network.

---

[9] "How Iran Moves Sanctioned Oil Around the World," *Reuters*, January 7, 2025, https://www.reuters.com/graphics/IRAN-OIL/zjpqngedmvx/.

## Illicit Financial Flows and Qatar's Alleged Role

While the physical smuggling of oil is one side of the coin, Prana's leaks also expose the financial circuits that clean and channel the profits back to Iran's military. According to U.S. Treasury findings (affirmed by Prana's intel), the AFGS and IRGC funnel oil revenues through a "shadow banking" structure of foreign exchange houses and front companies. The SEJ network, for instance, sold oil to refiners in China in exchange for payments routed through overseas shell accounts and commodity swaps. Cryptocurrency and alternative assets are increasingly used to settle these sanctions-evading trades. Notably, Prana discovered evidence of payment in gold bullion for Iranian exports. In one sensational revelation, the hackers unearthed documents indicating that Russia paid Iran approximately $1.75 billion in gold for a weapons deal[10] [11]– shipping over two tonnes of gold to the IRGC's front company (Sahara Thunder) as payment for 6,000 Shahed-136 drones. While that deal pertained to arms, not oil, it underscores the broader point: Tehran's illicit networks often transact outside conventional banking to avoid detection. Hard commodities like gold, cryptocurrencies, and bartered goods form a parallel value transfer system supporting sanctioned Iranian entities. Western officials believe similar methods are used for oil revenue: for example, a portion of Iranian oil sales to Asia may be paid via intermediaries in cash or crypto, or by offset agreements (barter of goods/services) that complicate tracking.

The Prana leaks also hint at high-level efforts to retrieve frozen funds and exploit international financial loopholes. In March 2025, *Der Spiegel* reported that an Iranian oil official traveled to Luxembourg to covertly unfreeze $1.6 billion in blocked assets held by Clearstream (a Deutsche Börse subsidiary).[12] A leaked passport image in Prana's trove revealed that this emissary was Majid Azami himself. In other words, the very mastermind of SEJ attempted to siphon sanctioned Iranian monies out of a European financial institution, presumably by presenting documents to claim the funds. (He was unsuccessful, as German authorities flagged the effort.) This incident illustrates the brazen lengths Tehran's network will go – from smuggling barrels at sea to scheming in foreign boardrooms – to generate and access cash for the regime. It also highlights why financial intelligence units must remain vigilant about unconventional moves, such as sudden legal appeals to release frozen accounts or surges in commodity transfers linked to Iran.

---

[10] "Russia paid Iran 'in gold bullion' for drones used in attacks on Ukraine," *The Telegraph*, February 7, 2024, https://www.telegraph.co.uk/world-news/2024/02/07/russia-paid-billions-gold-bullion-shahed-drones-ukraine-war/.

[11] "Gold for Drones: Massive Leak Reveals the Iranian Shahed Project," *Haaretz*, February 21, 2024, https://www.haaretz.com/israel-news/security-aviation/2024-02-21/ty-article-magazine/gold-for-drones-massive-leak-reveals-the-iranian-shahed-project-in-russia/0000018d-bb85-dd5e-a59d-ffb729890000.

[12] **"Military Funding: Iran Seeks to Access Billions in Frozen Hard Currency,"** *Der Spiegel*, March 6, 2025, https://www.spiegel.de/international/world/military-funding-iran-seeks-to-access-billions-in-frozen-hard-currency-a-d9fbf1de-e5a4-4a59-a845-b52469203aa1.

A particularly sensitive aspect of Prana's findings is the alleged involvement of Qatar. Prana-affiliated sources claim that elements of the Qatari state or businesses have "teamed up" with Iran to help circumvent U.S. sanctions by covertly selling Iranian oil. While details are sparse in the leaked files, this allegation has raised eyebrows given Qatar's geopolitical position. Qatar shares the giant South Pars/North Dome gas field with Iran and maintains relatively cordial ties with Tehran. Observers note that during the 2017–2021 Gulf diplomatic rift, Iran increased energy cooperation with isolated Qatar, potentially including shared oil storage or swap arrangements. It is conceivable that Iranian oil has been blended with Qatari hydrocarbons or funneled through Qatari-led ventures to mask its origin – effectively using Qatar as a conduit. Another possibility is that Qatari financial institutions or intermediaries facilitated payments for Iranian oil under cover of legitimate energy dealings. No official accusation has been made by the U.S. against Qatar on this front, but the hacktivist disclosures have prompted calls for scrutiny. If Qatari entities knowingly abetted Iran's evasion (for example, by issuing falsified certificates of origin or ignoring sanctions red flags in transactions), it would represent a serious corruption risk and breach of sanctions. Qatari officials have not addressed these specific allegations, and further investigation is needed to substantiate Prana's claims. Nonetheless, the mere suggestion of Qatar's involvement is significant – it points to Iran's ability to enlist even U.S.-allied states in its sanctions-busting, via backdoor deals and perhaps under-the-table incentives. For security agencies, this means monitoring not just traditional adversaries like China or Turkey in Iran's oil trade, but also friendly nations where Iranian and local interests quietly intersect.

## Assessment of Data Credibility and Impact

The information exposed by Prana Network is extensive and in many cases corroborated by independent sources. Reuters journalists, given access to the Sahara Thunder email cache, verified key details such as the ship-to-ship transfers, fake bills of lading, and involvement of Iran's Ministry of Defense and Armed Forces Logistics (MODAFL). The U.S. Treasury's subsequent designation of Sahara Thunder in April 2024 – labeling it a "front company" for Iran's government supporting the IRGC's shipping network – aligns exactly with Prana's revelations.[13] Likewise, the U.S. OFAC sanctions of November 29, 2023, which targeted SEJ, Majid Azami, and associates, prefigured much of what the SEJ hack later confirmed: that SEJ was funneling oil money to the AFGS and IRGC-QF. This convergence of Prana's leaked evidence with official actions suggests a high degree of reliability. In Germany, authorities appeared to act on intelligence similar to Prana's when thwarting Azami's attempt to withdraw the Clearstream funds. And media outlets from JNS to Iran International have used the leaks to augment their reporting on Iran's illicit oil trade. In short, Prana's data dumps have proven credible enough that governments are responding, whether through sanctions or investigations.

---

[13] **U.S. Department of the Treasury**, "Treasury Targets Networks Facilitating Illicit Trade and UAV Transfers on Behalf of Iranian Military," *Press Release*, April 18, 2024, https://home.treasury.gov/news/press-releases/jy2295.

That said, as with any leaked material, caution is warranted. The hackers have an anti-Iran regime agenda, so there is a possibility of selective release (emphasizing data that implicates Tehran while perhaps withholding context). Intelligence agencies are cross-checking the leaks with their own classified sources to fill any gaps or correct discrepancies. Thus far, no substantive contradictions have emerged; rather, Prana's leaks have enhanced outside knowledge of Iran's sanction-evasion in granular detail. The breadth of sources – from internal emails to contractual drafts – provides a multidimensional view that is hard to fabricate entirely. Moreover, Prana has now built a track record of successful operations (including hacks on Iranian drone programs and other IRGC fronts), which bolsters their credibility among analysts. Still, officials treat hacked data with caution: forensic analyses are underway to ensure none of the leaked documents have been doctored. Thus far, the consensus is that the materials are authentic and extremely valuable for mapping Iran's oil smuggling enterprise.

# Recommendations for Countering the Sanctions Evasion Network

The Prana leaks offer actionable intelligence for the United Kingdom and its allies to dismantle Iran's covert sanctions-evasion infrastructure. Leveraging these insights through targeted enforcement, diplomatic pressure, and interagency collaboration can significantly curtail the illicit oil revenues funding Iran's military-industrial complex.

## Sanction the Full SEJ Network

The UK's Office of Financial Sanctions Implementation (OFSI) should move in coordination with the FCDO and intelligence partners to:

- **Designate all entities and individuals** tied to Sepehr Energy Jahan (SEJ) and its affiliates, including unsanctioned board members, ship owners, and facilitators based in the UAE, India, and Southeast Asia.
- **Expand sanctions listings** under the Iran (Sanctions) Regulations 2023 and relevant UN-mandated arms embargoes.
- Ensure that names sanctioned by the U.S. and EU are mirrored in the UK's Consolidated List of Financial Sanctions Targets.
- **Encourage the EU and Five Eyes allies** to blacklist these actors simultaneously, denying them access to international finance and port services.

## Disrupt and Dismantle Shell Company Logistics

The UK should deploy its capabilities in corporate transparency and maritime oversight to:

- **Work with the Registrar of Companies (Companies House)** to identify and deregister UK-incorporated shell entities linked to Iranian oil trades.

- **Press Crown Dependencies and Overseas Territories** to cooperate fully with UK authorities in cracking down on front companies exploiting gaps in beneficial ownership disclosure.
- **Advocate at the IMO and G7 for enforcement mechanisms** against flags of convenience (notably Panama and Tanzania) used by Iran's ghost fleet.
- **Issue joint HM Treasury–Department for Transport advisories** to UK-based insurers, classification societies, and shipping firms outlining red-flag indicators – including AIS manipulation, repeated flag-hopping, and ship-to-ship transfers in high-risk zones.
- **Support seizures and forfeitures of vessels** under UK law, using the Proceeds of Crime Act 2002 (POCA) where applicable, and in concert with allied navies under maritime interdiction regimes.

## Enhance Monitoring of Illicit Financial Flows

UK financial and intelligence bodies – notably the National Crime Agency (NCA), Serious Fraud Office (SFO), and HMRC – should:

- **Mine the Prana leaks** for financial data points, including SWIFT accounts, crypto wallets, and commodity traders laundering oil revenues.
- **Collaborate with the Financial Conduct Authority (FCA)** and major UK banks to flag suspicious large-volume transactions tied to Tether, Bitcoin, or other digital assets associated with Iranian-linked exchanges.
- **Work through the Financial Action Task Force (FATF)** to tighten scrutiny on jurisdictions implicated in trade-based money laundering schemes tied to Iranian oil, especially involving gold and other hard commodities.
- **Expand outreach to precious metals dealers and logistics firms** under the Money Laundering Regulations (MLR 2017) to enhance vigilance over bulk shipments of gold bullion and other assets that may be used for barter-style payments.

## Engage and Pressure Complicit States – Including Qatar

The UK should use its diplomatic weight to:

- **Raise concerns with Qatari officials** over allegations of Doha-based facilitation of IRGC-linked finance and meetings. Quiet engagement through diplomatic channels can verify and pressure corrective actions without destabilising broader UK-Qatar relations.
- **Encourage Middle Eastern partners (UAE, Oman, Bahrain)** to act on intelligence identifying Iranian front companies operating in their jurisdictions, sharing select insights from the Prana leaks.
- **Lead EU+ dialogues with Asian counterparts**, especially Singapore, Malaysia, and China, where Iranian oil reaches its end markets. Targeted sanctions and reputational costs for Chinese refiners knowingly accepting Iranian crude should be explored multilaterally.

## Strengthen Maritime Domain Awareness and Enforcement Tools

The UK should invest in strategic maritime capabilities to:

- **Leverage satellite monitoring and AI analytics** via the Royal Navy's Maritime Domain Awareness (MDA) framework, especially in the Strait of Hormuz, Red Sea, and South China Sea.
- **Enhance collaboration with Lloyd's maritime intelligence services** and open-source tracking platforms to detect spoofing patterns, "dark fleet" movements, and ghost ship clusters.
- **Push for IMO reforms** to require stricter reporting and disclosure on vessel identity changes, and impose penalties on flag registries linked to habitual evasion.
- **Explore the legality of interdiction partnerships** under international maritime law and counter-terrorism statutes, modelled on U.S. civil forfeiture actions, to seize Iranian-linked cargos en route to UK-allied ports.

## Leverage Intelligence from Prana for Offensive Countermeasures

UK intelligence and enforcement agencies – including MI6, GCHQ, and the NCA – should:

- **Exploit Prana's leaked data** to identify facilitators, brokers, intermediaries, and service providers linked to the SEJ network and Sahara Thunder.
- **Coordinate cyber and HUMINT operations** to monitor or disrupt the digital infrastructure of key entities involved in sanctions evasion.
- **Establish secure reporting channels** to engage OSINT researchers and independent cyber investigators contributing to transparency efforts.
- **Consider limited engagement with hacktivist-led findings**, ensuring information is vetted and integrated into ongoing financial crime and terrorism financing investigations.

## UK Leadership on Sanctions Enforcement

The UK has the regulatory tools, diplomatic reach, and intelligence capacity to play a leading role in exposing and dismantling Iran's oil smuggling network. By operationalising the Prana revelations through robust enforcement, financial scrutiny, and diplomatic coordination, the UK can:

- Disrupt Iran's revenue streams for regional militancy and WMD proliferation.
- Bolster the credibility of international sanctions regimes.
- Demonstrate global leadership in defending the rules-based order.

As the Prana leaks affirm, "the corrupt should fear us as the truth empowers the oppressed." The UK must now ensure that truth is turned into meaningful, strategic action.