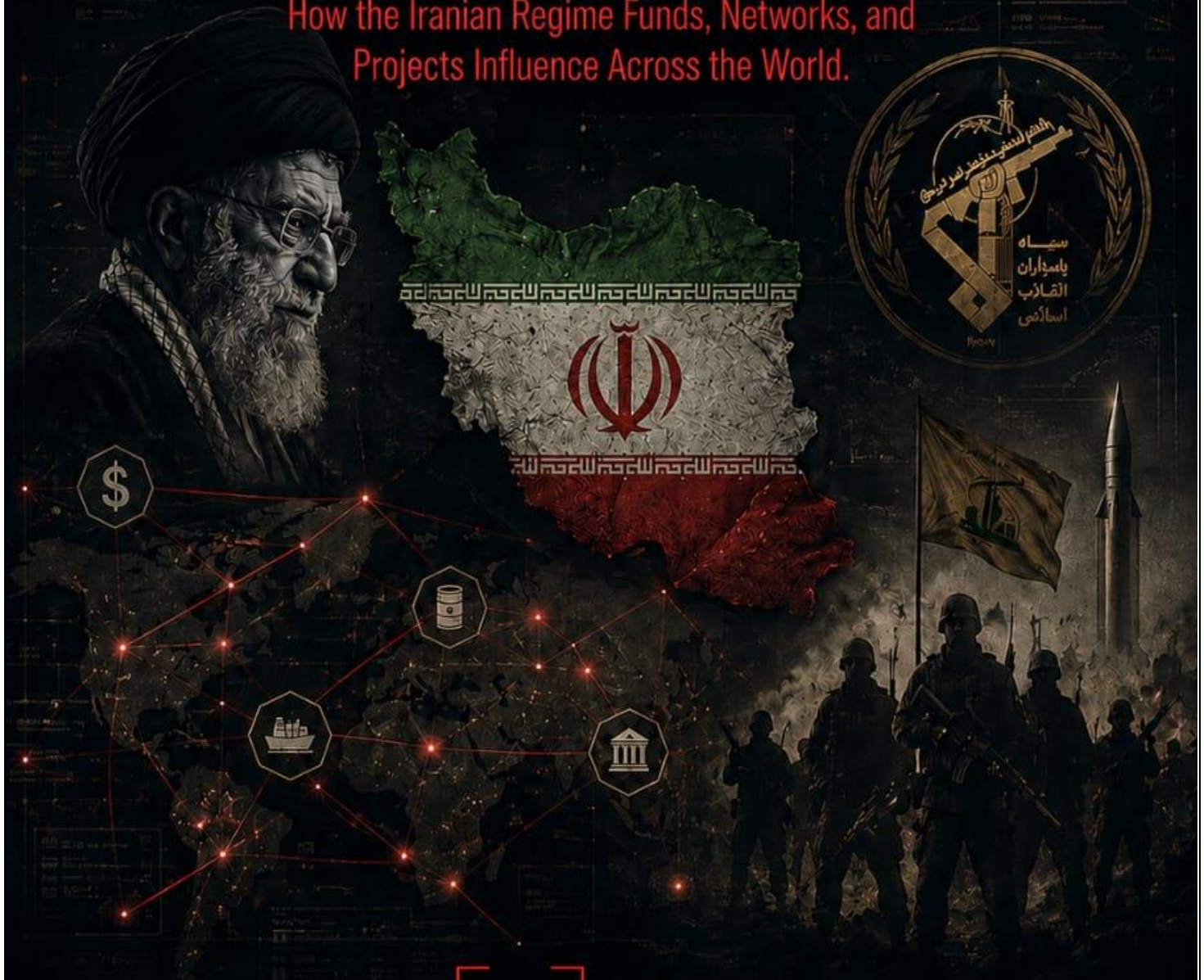
SOUTH BLOC REPORTS

OPEN SOURCE INVESTIGATIVE REPORT

THE SHADOW EMPIRE

An Open-Source Reporting Investigation into How the Iranian Regime Funds, Networks, and Projects Influence Across the World.



SBR SOUTH BLOC REPORTS

southblocreports.in | @SouthBlocReports

SOUTH BLOC REPORTS
Published by South Bloc Reports

The Shadow Empire, an Open Source Investigation Into How the Iranian Regime Funds, Networks, and Projects Influence Across The World

INDEX

SHADOW OPERATORS - AGENTS OF IRAN

The Iranian regime uses a highly aggressive use of dual-citizens, paid criminal proxies, and local traitors to steal military data, coordinate arms sales, and track human targets on global streets. The regime utilizes deep-cover individuals inside Western nations to bypass international weapons bans and gather intelligence on high-value targets. American Federal Agents on April 18, 2026 at Los Angeles International Airport (LAX) arrested Shamim Mafi, the 44 year-Old Iranian national and U.S. lawful permanent resident living in the Woodland Hills, California. For ten years, Shamim Mafi operated below the radar, travelling frequently between U.S., Turkey, and Iran. Her technical mandate was acting as an international logistics broker: she actively arranged the sale of Iranian-made military drones, bombs, bomb fuses, and millions of rounds of live ammunition directly to Sudan.

In Europe, the regime uses sleeper networks to target political individuals and Jewish communities. British Counter-Terrorism police launched early-morning raids across Barnet, Watford, and Harrow on March 6, 2026 at London's northern regions, arresting four men, one Iranian national and three dual British-Iranian citizens. This cell was caught conducting ground surveillance routines and photographing targets within the local Jewish community. This operation followed a parallel pattern in Denmark, where a suspected Iranian operative was arrested for gathering granular operational intelligence on Berlin’s Jewish community to pass back to Tehran.

The most severe technical penetration involves the regime recruiting local Israeli citizens, security personnel, and military engineers through financial bribery to compromise defense infrastructure from the inside. The Air Force and Iron Dome Infiltration: Security services arrested two Israeli Air Force engineers on direct espionage charges for selling classified technical blueprints to Iranian handlers. This was backed by the separate indictment of an active-duty Iron Dome reservist soldier who passed sensitive operational layouts of Israel's primary air defense batteries directly to Tehran. In a massive security failure, a ring of seven Jewish-Israelis was busted after spending months mapping out IDF bases, military installations, and security figures on behalf of Iran. Another cell of three Israelis was caught executing specific logistical tasks assigned by Iranian intelligence. The regime's agents targeted the top tier of Israeli leadership. Local resident of the Galilee was arrested for gathering intelligence on former Defense Minister Yoav Gallant. In another separate case, an

Israeli-American suspect was detained for tracking the movements of far-right Minister Itamar Ben-Gvir and a former IDF chief. To test their agents' loyalty, Iranian handlers frequently ordered low-level tasks first—such as an operative arrested in Holon who was paid to film the private home of former Prime Minister Naftali Bennett.

Regime's intelligence ministries do not limit their operations to Western or Israeli soil - they aggressively build networks inside Arab nations and European borders to monitor military assets and plan to sabotage accordingly. Qatari Security officials in March 2026 officially announced the arrest of two active IRGC sleeper cells spying inside the country, alongside three operatives caught with equipment intended for local sabotage. This came as regional security grids tightened following wave-style drone attacks on Gulf energy facilities. The Iranian Ministry of Intelligence (MOIS) uses political refugee covers to infiltrate Europe. In Albania, local counter-espionage forces arrested a documented MOIS agent working under a fake humanitarian cover to track exiled Iranian dissidents. These intelligence-gathering operations are designed to build a permanent, actionable target database. This was exposed firsthand when the Mossad intercepted and captured an active Iranian-hired assassin inside Iran, extracting a full video confession detailing a dismantled plot to assassinate Israeli businessmen and British military personnel stationed at strategic bases in Cyprus.

MONEY LAUNDERING AND HAWALA NETWORKS

The Iranian regime operates a multi-billion-dollar banking ecosystem that weaponizes cash brokers, compromised global banking giants, front businesses and cryptocurrency to bypass international sanctions. To funnel cash directly into Western cities, the Islamic Revolutionary Guard Corps (IRGC) embeds its financial agents inside seemingly normal, everyday street-front businesses. In the United Kingdom, counter-financial crime operations unmasked a local carpet shop in London and multiple local mini-markets in Yorkshire acting as active hubs for an Iranian money laundering apparatus. On paper, these locations sold household goods; under the surface, they pooled local cash to blend and obscure black-market funds.

This brick-and-mortar front strategy spans the globe. In Canada, federal investigations into Toronto and Greater Toronto Area (GTA) crypto shops unmasked deep-cover finance cells tied to Salim Henareh, a Toronto-based businessman entangled in massive sanctions-evasion networks. These setups systematically violate Anti-Money Laundering (AML) controls to pass funds directly to proxy networks. To keep this money untraceable, the regime relies heavily on Hawala—a trust-based network operating entirely outside of digital banking lines. In a massive April 2026 bust, Pakistan's Federal Investigation Agency (FIA) seized over Rs. 2 billion alongside stacks of raw Iranian currency, totally dismantling a major regional Hawala cell functioning as a direct artery for the IRGC.

The financial lifeblood of the regime is illicit oil, which requires a vast corporate masking system to enter the clean global economy. The IRGC coordinates a massive "shadow fleet" of unregistered tankers that transport oil to small, independent "teapot refineries" in East Asia. The resulting profits are washed through a global corporate shell machine designed to look completely disconnected from Tehran.A digital trail recently unmasked an intricate IRGC money machine hiding behind fake corporate assets, including a stock-footage CEO and a shell company named Petrochemical Commercial Company (PCC). Operating directly out of offices in the heart of London, PCC utilized major international banking platforms—including standard accounts at HSBC and Standard Chartered—to move millions of dollars across the globe before international regulators flagged the activity. This structural evasion is mirrored across Western Europe, where the Federal Financial Supervisory Authority (BaFin) in Germany launched an intensive probe into a small, specialized bank in Hamburg suspected of functioning as an active, direct financial clearinghouse for Iranian-backed operations.

When small shell companies are not enough, the Iranian state relies on direct collusion with foreign state-owned banks and vulnerable financial systems to clear billions of dollars at a time. The most prominent example of this institutional evasion is Turkey's state-owned Halkbank, which was dragged into federal court in New York for orchestrating a massive, multi-billion-dollar "gas-for-gold" scheme that allowed the Turkish financial system to process illegal payments for Tehran with high-level political cover. Beyond traditional banking, the regime has rapidly adapted to digital currencies to fund its armed regional networks, specifically bypassing global watchdogs like the Financial Action Task Force (FATF), which maintains Iran on its absolute highest-risk blacklist.

When traditional routes tightened, Hamas and the Houthis turned directly to digital assets, using crypto platforms to receive millions from Tehran. Global giants like Binance faced massive internal turmoil and federal firings after it was discovered that staff members and specialized internal setups allowed billions in transactions to slip through directly to Iranian users despite strict global blockades. The financial tightening has sparked heavy international pushback. The U.S. issued strict warnings to Swiss wealth managers like Swiss Bank Maerki Baumann over potential financial system bans, while the United Arab Emirates (UAE) launched a sweeping, aggressive crackdown, freezing accounts and completely dismantling an intricate Dubai-based financial ring that was actively laundering millions directly to Hezbollah.

CRIMINAL NETWORK - MUSCLE FOR HIRE

The regime actively outsources its crime work, including targeted assassinations, embassy bombings, and target of political and religious commentators, to violent street gangs, drug cartels, and organized crime syndicates across Europe and the Americas. Faced with tight monitoring by Western intelligence agencies, the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence (MOIS) have pivoted to a strategy of "strategic outsourcing." Instead of sending traditional Iranian agents to pull triggers, Tehran hires local, violent criminal networks to execute high-profile hits. This dynamic was explicitly exposed by the Mossad and European security services following a series of violent attacks, including gunshots and grenade deployments, targeting the Israeli Embassies in Stockholm, Sweden, and Copenhagen, Denmark. The primary proxy for these European operations is Foxtrot, one of Sweden's most lethal and fractured drug cartels, alongside its fierce rival network, Rumba.

The regime secured absolute loyalty from Foxtrot's top leadership, including notorious crime boss Rawa Majid (known as the "Kurdish Fox"). When Majid fled international arrest warrants, the regime granted him safe haven inside Iran. In exchange for this protection, his cartel became a fully operational hit squad for Tehran on European soil. To avoid direct legal links, the Foxtrot-Iran axis utilizes digital messaging apps to recruit local street-level assets. Swedish court in April 2026 put five minors on trial for their direct involvement in an Iran-directed murder plot targeting a prominent political commentator. This case exposed a highly disturbing operational thinking - the regime deliberately hires teenagers and minors to perform surveillance and carry out contract killings because they face less severe legal penalties under European juvenile laws.

This criminal alliance extends directly into the Western Hemisphere, where the regime has woven itself tightly into the fabric of South American drug networks to establish a permanent asymmetric launch pad against the United States.

In Bolivia, the IRGC has successfully constructed a secure "cocaine drone corridor," partnering with local syndicates to manage transport hubs while building long-term logistics infrastructure. This pipeline runs all the way north to America's southern border, where U.S. counter-narcotics and intelligence agencies are scrambling to track the growing coordination between Iranian handlers and major Mexican drug cartels. The lethal nature of this network inside the United States was put on full public display during federal court proceedings in

New York. Two high-profile mobsters affiliated with an Eastern European organized crime syndicate were found guilty of accepting direct payments from Iranian intelligence operatives to plan the assassination of prominent Iranian-American journalist and dissident Masih Alinejad at her residence in Brooklyn. The plotters bypassed standard international security nets by operating through a web of independent gang cells, showing that the regime's espionage network inside America is significantly bolder and deeper than standard diplomatic indicators suggest.

The sheer scale of this state-sponsored criminal footprint has forced major Western powers to adjust their legal counter-measures. The United Kingdom officially upgraded its sanctions regime, levying severe individual and corporate designations directly against prominent actors within the Iranian organized crime network. This coordinated push was mirrored by the U.S. Treasury, which issued sweeping sanctions targeting the Foxtrot gang and its leadership for acting as direct geopolitical extensions of the state in Tehran. Intelligence analysts at institutions like West Point's Combating Terrorism Center (CTC) and the Atlantic Council argue that these traditional financial freezes are no longer enough to blunt the threat. Because the regime completely weaponizes illicit global markets to maintain its operations under pressure, there is a mounting, unified push from security officials to officially designate these Iran-linked criminal proxy networks as Foreign Terrorist Organizations (FTOs). Treating these cartels as national security threats rather than standard street-level police matters remains the only way to dismantle Tehran's homeland option for foreign sabotage.

DIGITAL CYBERCRIME

The Iranian regime systematically weaponizes state-sponsored hacking groups, corporate tech fronts and destructive ransom ware networks to breach Western critical infrastructure, steal military secrets, and run multi-million-dollar networks. The Iranian Ministry of Intelligence and Security (MOIS) and the IRGC have completely blurred the difference between state sponsored espionage and common street cybercrime. Instead of hacking under the Iranian flag, state-backed spies disguise their operations as private, profit-driven ransom ware gangs. Security research from Check Point and Palo Alto Networks (Unit 42) exposed that groups like MuddyWater and Peach Sandstorm (APT33) execute complex "false flag" operations. Deploying destructive wiper malware like Pay2Key or Chaos variants—and leave behind ransom notes demanding crypto currency.This is a deliberate psychological camouflage. On the surface, it looks like a simple digital shakedown by independent criminals. In reality, the primary goal is not money; it is the total destruction of commercial data, permanent disruption of Western services, and absolute deniability for Tehran. These groups use advanced social engineering to lure targets. In Western Europe, state-backed operatives built highly polished, fake digital personas posing as independent experts on Middle Eastern policy or technical recruiters offering lucrative corporate positions. Using these covers, they targeted and successfully breached European industrial executives, defense firms, and even a prominent German politician.

The threat from these state-sanctioned actors has officially shifted from simple website defacement to highly complex, physical threats targeting the essential services that ordinary citizens rely on. Joint alerts issued by FBI, NSA, CISA, and the UK National Cyber Security Centre (NCSC) have directly warned that Iranian cyber networks are aggressively scanning and exploiting known vulnerabilities in widespread corporate software, specifically the unpatched Microsoft Exchange, Microsoft Intune, and Fortinet flaws for them to gain backdoors into the Western industries. In a severe display, a coordinated Iranian-linked attack hit critical healthcare infrastructure, deploying severe wiper malware against the Stryker network and connected hospitals in Cork. The breach forced healthcare facilities to lock down emergency systems and scramble to protect life-saving medical devices. Iranian state actors have successfully breached American municipal drinking water grids, targeting vulnerable Industrial Control Systems (ICS) and Operational Technology (OT) that keep civic utilities safe. The regime's hackers deployed a massive ransomware shakedown utilizing

Ubuntu-based DDoS tools that crippled the Los Angeles mass transit system. They have similarly claimed credit for sudden digital disruptions targeting consumer networks like Chime and Pinterest, while regional security groups in the Gulf tracked a massive eight-fold surge in Iranian cyber operations actively aiming to blind IP security cameras and sabotage energy companies across Saudi Arabia and the UAE.

This global cyber war is made possible by legitimate-looking domestic tech companies acting as operational shields inside Iran. U.S. Department of Justice and corporate investigators showcased state-controlled tech fronts, including an Iranian company named Cloudzy, which provided the vital virtual private server (VPS) architecture used by advanced persistent threat (APT) groups like the Ajax Security Team. These entities operate out of secure digital sanctuaries, evading Western sanctions by selling untraceable infrastructure to state hackers who deploy tools like the Tickler malware. The high-level scale of the threat has forced an aggressive international response. The United States government has placed a massive $10 million reward on the heads of top Iranian cyber operatives, the DOJ has executed counter-operations to disrupt known sleeper cells and dismantle hacker infrastructure. This defensive frontline has expanded into Europe, where the UK National Crime Agency (NCA) arrested a key Iranian national who was actively running a massive, illegal payment platform designed specifically to wash cash for international cybercriminals. From password-spraying attacks on Microsoft 365 accounts to the direct targeting of senior federal intelligence emails, the regime's cyber network remains a premier threat to global stability.

IDEOLOGICAL JIHAD AND RADICALISATION

The Iranian regime exports its radical expansionist ideology across Europe, North America, and Asia, using state-backed religious centres, online radicalization campaigns and local sleeper cells to cultivate domestic extremism. The geopolitical criris from the ongoing multi-front war with Iran has triggered an aggressive, coordinated increase in state-backed Islamist extremism across the West. Europol and senior European security officials officially warned that the will face an elevated, high-risk terrorism threat directly fueled by Tehran. This assessment is backed by data - while global terrorism numbers hit a decade low, Western fatalities and active terror plots have surged dramatically due to pro-Iranian criminal operations.

In United Kingdom, police and counter-terrorism units logged a direct Iranian-linked operation involving low-level arson campaigns, decisive in the firebombing of local emergency vehicles and ambulances in the Jewish community of Golders Green, London. In Belgium, federal investigators discovered an active network of pro-Iranian sleeper cells stockpiling tactical assets. The cells aimed to attack Jewish community centers and prominent public places to openly demonstrate their capability to act under direct orders from Iran. U.S. counter-terrorism agencies in March 2026 investigated a series of plots tied to homegrown cells in Michigan and Old Dominion. Adding to this, federal prosecutors in Brooklyn brought a massive murder-for-hire terrorism trial exposing an Iranian-backed conspiracy specifically designed to assassinate high-profile political figures on American soil, including Donald Trump.

To recruit and radicalize assets on foreign soil, the regime exploits Western democratic protections by embedding intelligence handlers inside seemingly normal religious and cultural institutions. This massive ideological network suffered a huge blow when German federal authorities officially banned the Islamic Centre Hamburg (IZH) and its networks. German intelligence showcased IZH not as a local community hub, but as a direct outpost of the Iranian state, actively spreading anti-democratic propaganda, supporting Hezbollah, and mapping out potential targets across Western Europe.

This strategy of using state-funded outposts to capture local populations is a core pillar of the IRGC's global expansionist doctrine. Where physical infrastructure is restricted, the regime relies heavily on aggressive digital operations to export its brand of Jihad. In India, local intelligence and security agencies flagged a major online radicalization push. Using specialized social media channels, Iranian digital cells actively exploit Middle Eastern conflicts to manufacture local grievances and radicalize domestic Shia youth. This digital and logistical pipeline has forced international checkpoints into high alert. In Singapore, Home Affairs Minister K. Shanmugam announced a heavy increase in security checkpoints due to rising spill over risks from the Iran war. This followed intense monitoring of regional travel routes, specifically concerning Malaysia's historic logistical role in allowing sanctioned Iranian intelligence entities and financial networks to operate freely within its borders.

The ideological pressure stems directly from the top tier of the ruling apparatus in Tehran. In early 2026, the Iranian Parliament went as far as issuing an official, public declaration warning of a mandatory, global Jihad if the regime's supreme leadership faces direct military targeting by Western forces. This top-down command filters down into extensive psychological influence campaigns designed to destabilize foreign civil societies. Security analysts at the Jerusalem Centre for Foreign Affairs (JCFA) tracked a huge surge in coordinated Iranian state media narratives engineered to amplify social divisions, manipulate the public opinion and directly spark unrest across U.S. university campuses. By providing ideological backing, talking points and motivation to elements worldwide, the regime successfully converts its radical domestic theology into a highly volatile tool for global asymmetric warfare.

MANUFACTURING CHAOS - PROTEST FUNDING

The Iranian regime covertly finances, directs and manipulates domestic protest movements across the United States and Europe, weaponizing local political issues to create chaos Western cities and destabilize foreign civil societies. The interference of the Iranian state in Western public protests is not a matter of speculation- it is an active, documented finding verified by the highest levels of the United States intelligence. Direct public warnings issued by the Director of National Intelligence (DNI) openly confirmed that Iranian government actors are aggressively seeking to exploit, support, and fund domestic political movements. According to these intelligence findings, the regime covert intelligence networks actively track the ongoing social debates and insert themselves directly into the planning of these demonstrations. The primary objective is to amplify social divisions, reduce public trust in democratic institutions and push targeted foreign policy decisions that benefit Iran's regional agenda. By masquerading as local grassroots activists, Iranian intelligence operatives successfully hide the hand of the state while using Western citizens to project their political influence.

The primary targets for this foreign influence apparatus are elite Western university campuses and high-profile activist infrastructure. Intelligence tracking indicates that Iranian-linked entities provide direct financial support to fringe groups organizing anti-Israel and pro-Hamas demonstrations. This includes funding the purchase of camping gear, bulk supplies, and professional signage used to construct long-term protest encampments that paralyzed premier American universities.

The Digital Puppeteers: Behind the scenes, Iranian cyber and psychological operations teams pose as normal American citizens on social media platforms. They actively contact local student organizers, coordinate logistics for street-level marches, and push specific radical talking points designed to prevent any peaceful compromises or dialogue on campus.

This financial and operational pipeline stretches directly into Europe. UK Home Office launched intensive investigations into prominent activist networks, most notably Palestine Action. Amid a mounting government push to officially ban the organization as a national security threat, intelligence services closely monitored the group's financial backing following disruptions at defense manufacturing sites, tracking Iranian connections designed to sabotage British industry from the inside. To support these street-level operations, the

regime runs a massive, synchronized international propaganda network. State media outlets like Press TV and digital bot farms under the control of the IRGC aggressively film, edit, and distribute footage of Western protest clashes to a global audience.

This media campaign serves a dual purpose. For domestic audiences inside Iran, the regime uses images of Western police lines and campus arrests to falsely claim that Western democracies are collapsing and that the entire world supports the regime's ideological stances. For international audiences, they use highly polished English-language content to twist standard geopolitical realities, hiding their extensive record of domestic executions and severe human rights abuses against the Iranian population behind a fake shield of international human rights advocacy. This calculated exploitation of Western free speech allows a hostile dictatorship to buy direct influence on the streets of London and Washington.

NARCOTIC PIPELINE

The Iranian regime global drug trafficking acts as an official state industry, weaponizing international narcotics pipelines to generate billions in untraceable foreign currency, destabilize enemy nations and finance armed proxy networks. The Islamic Revolutionary Guard Corps (IRGC) does not limit its drug operations to the Middle East - it builds direct, high-level business connections with the world's most powerful, violent transnational cartels to funnel massive shipments into Western Europe. This reality was exposed by Detective Chief Superintendent Seamus Boland, the head of Ireland's Garda National Drugs and Organised Crime Bureau. Irish and international investigators uncovered direct links between the notorious Kinahan Organised Crime Group (KOCG)—a global 1.5-billion-euro syndicate and corporate structures located directly inside Iran.

This transnational axis was brought into sharp focus following Ireland's largest cocaine seizure in history on the bulk cargo ship MV Matthew. Elite Irish Army Rangers stormed the vessel at gunpoint off the Cork coast, seizing 2.25 tons of high-purity cocaine valued at over €157 million. An Irish Special Criminal Court sentenced the ship's former captain, Soheil Jelveh, and senior officer Saied Hassani—both Iranian nationals—to 17.5 and 15 years in prison, respectively. Court records stated that Iranian maritime officers were operating under the remote coordination of "Captain Noah" identified as Mehdi Bordbar, a Dubai-based Hezbollah member. The operation utilized Venezuelan shipping ports to load the cargo under the cover of night, demonstrating how Iranian state proxy elements and European criminal syndicates share logistics to finance foreign operations.

In the Middle East, the regime uses the synthetic drug trade as a physical weapon against neighboring Arab states, primarily targeting the Gulf kingdoms and Jordan. The primary narcotic in this region is Captagon, a highly addictive amphetamine mass-produced in the industrial-scale labs throughout regime-controlled areas of Syria and parts of Lebanon under the direct protection of Hezbollah and the IRGC. This multi-billion-dollar trade has forced Jordan into an active border war. The Jordanian Armed Forces have drastically intensified their border deployment along the Syria, engaging in frequent firefights with drug-smuggling militias backed by Iran. These smugglers use military equipment, including armed drones, night-vision gear, and armored vehicles, to push millions of Captagon pills and heavy shipments of weapons into Jordan for onward transit to Saudi Arabia. This pipeline fulfills a

two purpose - it generates massive liquidity to bypass Western economic sanctions while systematically undermining the internal security and social fabric of regional adversaries.

The regime manages a massive global pipeline for heroin and methamphetamine, exploiting its domestic transport hubs, state-managed ports and agricultural resources to push drugs out to the international market. Rather than relying on expensive chemical imports, IRGC weaponized the natural growth of the Ephedra plant in neighboring Afghanistan. Iranian cartels systematically process this raw plant material inside domestic labs to manufacture massive volumes of cheap, highly potent crystal methamphetamine, which they route directly toward high-value markets in Australia and Southeast Asia via transit hubs like Malaysia's Port Klang. The regime utilizes major commercial shipping networks to move industrial-scale quantities of Afghan-sourced heroin. In India, security agencies staged a monumental bust at Gujarat's Adani Port, intercepting thousands of kilograms of heroin masked as innocent talcum powder shipments originating from trading firms linked to Iran. his industrial masking strategy is identical on European land routes. Border authorities in Bulgaria seized 288 kilograms of heroin hidden inside a commercial truck arriving d from Iran. Italian customs police made a parallel multi-ton haul on a container ship departing from Iranian ports.

The ultimate irony of the regime's drug statecraft lies in the brutal treatment of its own domestic population. While the IRGC exports high-purity narcotics globally to accumulate foreign exchange, the domestic Iranian market is flooded with low-purity, highly toxic chemical trash. Local reports and data from groups like IranWire confirm that drug addiction rates inside Iran have surged to catastrophic levels, while the purity of street-level narcotics has crashed, causing thousands of fatal overdoses among the civilian population annually. The regime uses this domestic health crisis as a convenient tool of social control. While top-ranking IRGC generals have been formally flagged by Western intelligence agencies as primary kingpins of the regional drug trade, the judiciary in Tehran routinely rounds up and executes thousands of low-level, impoverished Iranian citizens for minor drug possession. This severe domestic hypocrisy shields the true state-level orchestrators, allowing the ruling elite to run a global cartel under the protection of sovereign diplomatic borders.

REFERENCES

- https://www.theguardian.com/us-news/2026/apr/19/woman-arrested-la-arms-trafficking-iran-africa
- https://www.aljazeera.com/news/2026/3/3/qatar-announces-arrest-of-iranian-irgc-sleeper-cells
- https://www.cbsnews.com/news/london-iran-war-spies-arrested-jewish-community/
- https://www.ynetnews.com/article/hkddlyf711e
- https://nypost.com/2026/04/19/us-news/iran-arms-suspect-arrested-at-lax-after-10-years-in-us/
- https://www.euronews.com/my-europe/2025/07/01/iranian-spy-suspect-arrested-in-denmark-for-gathering-info-on-berlins-jewish-community
- https://www.timesofisrael.com/jerusalem-man-arrested-to-be-charged-with-spying-for-iran/
- https://www.israelhayom.com/2026/04/06/4-idf-soldiers-arrested-on-suspicion-of-spying-for-iran/
- https://wanaen.com/two-israeli-air-force-engineers-arrested-on-espionage-charges-for-iran/
- https://www.timesofisrael.com/iron-dome-reservist-soldier-indicted-for-spying-for-iran/
- https://www.timesofisrael.com/israeli-charged-with-filming-ex-pm-bennetts-home-on-behalf-of-iran/
- https://www.ynetnews.com/article/bjlfzipmzx
- https://www.i24news.tv/en/news/israel/defense/artc-iran-linked-espionage-galilee-resident-arrested-for-intelligence-gathering-on-gallant
- https://www.jpost.com/israel-news/crime-in-israel/article-883423
- https://www.timesofisrael.com/two-holon-residents-arrested-on-suspicion-of-spying-for-iran/
- https://www.iranintl.com/en/202507076196
- https://www.timesofisrael.com/luring-in-israelis-of-all-types-iran-casts-about-in-hopes-of-snagging-quality-spies/
- https://www.timesofisrael.com/israeli-american-anti-zionist-suspected-of-spying-for-iran-on-ex-idf-chief-ben-gvir/
- https://www.timesofisrael.com/police-arrest-three-more-israelis-on-iran-espionage-suspicions/
- https://www.timesofisrael.com/police-arrest-three-more-people-suspected-of-spying-for-iran/
- https://www.ynetnews.com/article/rk2nvkhxxx
- https://www.iranintl.com/en/202306301395
- https://www.cnn.com/2024/12/13/middleeast/israel-alleged-spy-cells-iran-intl-cmd
- https://www.jpost.com/israel-news/crime-in-israel/article-859475
- https://www.tabletmag.com/sections/israel-middle-east/articles/iran-spy-ring-robert-malley-lee-smith
- https://www.reuters.com/world/middle-east/israel-breaks-up-another-iran-spy-ring-security-services-say-2024-10-31/
- https://www.nytimes.com/2024/10/21/world/middleeast/israel-iran-spying-arrests.html
- https://www.timesofisrael.com/mossad-says-it-caught-cyprus-terror-plot-assassin-in-iran-airs-clip-of-confession/
- https://www.timesofisrael.com/3-israelis-arrested-for-allegedly-carrying-out-tasks-for-iranian-intelligence-agents/
- https://www.timesofisrael.com/seven-jewish-israelis-arrested-for-spying-on-security-figures-idf-bases-for-iran/
- https://www.cbsnews.com/news/ice-arrests-11-iranian-nationals-48-hours/
- https://www.bbc.co.uk/news/articles/c5y5wy380g4o
- https://www.ncr-iran.org/en/ncri-statements/terrorism-fundamentalism/iranian-regime-intelligence-ministrys-agent-arrested-in-albania/
- https://www.lbc.co.uk/article/spy-arrested-plot-british-military-base-cyprus-rpXzC_2/

- https://www.jpost.com/israel-news/article-820919
- https://www.ncr-iran.org/en/uncategorized/irans-regime-agent-arrested-in-the-us-for-secretly-lobbying-for-the-iranian-regime/
- https://www.ibtimes.co.uk/iran-spy-arrests-who-are-two-men-charged-london-tehrans-secret-operations-1786651
- https://thehill.com/opinion/international/5876751-iran-hawala-networks-sanctions-evasion/
- https://nationalinterest.org/blog/middle-east-watch/how-the-uae-is-cracking-down-on-illicit-iranian-finance
- https://www.wionews.com/photos/-financial-assassins-how-uae-s-mbz-can-bankrupt-irgc-to-avenge-attack-on-dubai-and-abu-dhabi-1772363341925
- https://www.iranintl.com/en/202512079325
- https://www.news18.com/world/from-teapot-refineries-to-hawala-hubs-how-irgc-launders-oil-money-via-shadow-fleet-exclusive-ws-kl-9956871.html
- https://evrimagaci.org/gpt/iran-funnels-millions-to-hezbollah-through-dubai-network-518056
- https://www.wsj.com/world/middle-east/iranian-funds-for-hezbollah-are-flowing-through-dubai-85785a77
- https://gnet-research.org/2025/05/14/cash-flow-breaking-down-the-houthis-multibillion-dollar-financial-networks/
- https://www.wsj.com/world/middle-east/hamas-needed-a-new-way-to-get-money-from-iran-it-turned-to-crypto-739619aa
- https://www.arabnews.com/node/2059986/world
- https://www.yorkshirepost.co.uk/news/crime/iranian-man-arrested-in-yorkshire-in-connection-with-money-laundering-at-mini-markets-5304722
- https://www.thenationalnews.com/world/uk-news/2024/01/18/london-carpet-shop-used-in-iranian-money-laundering-operation/
- https://www.indiatoday.in/india/west/story/hawala-scam-fema-act-enforcement-directorate-uco-bank-229636-2014-12-03
- https://www.indiatoday.in/india/story/black-money-uco-bank-united-states-indo-iran-scam-hawala-240888-2015-02-18
- https://www.indiatoday.in/india/story/indo-iran-uco-bank-scam-cbi-registers-pe-against-unknown-rbi-officials-uco-bank-ex-official-324849-2016-05-21
- https://propakistani.pk/2026/04/22/fia-seizes-rs-2-billion-and-iranian-currency-in-major-hawala-bust/
- https://www.myjoyonline.com/hawala-method-this-network-enables-terrorists-to-launder-money-in-europe/
- https://globalinitiative.net/analysis/irans-criminal-statecraft-how-teheran-weaponizes-illicit-markets/
- https://www.amlintelligence.com/2020/11/leaked-watchdog-report-exposes-millions-transferred-illegally-from-iran-to-canada-violating-sanctions/
- https://civil.ge/archives/360602
- https://www.wsj.com/articles/recep-tayyip-erdogan-allowed-turkish-banks-to-help-iran-make-illegal-payments-witness-says-1512071333
- https://www.cbc.ca/news/politics/salim-henareh-cameron-ortis-case-alleged-money-laundering-1.6991409
- https://warontherocks.com/irans-cartel-strategy-the-islamic-revolutionary-guard-corps-in-the-western-hemisphere-2/
- https://www.iranintl.com/en/202605191058
- https://www.scmp.com/news/world/united-states-canada/article/3353200/us-treasury-department-tells-banks-flag-suspected-iranian-money-laundering-networks

- https://www.amlintelligence.com/2026/04/news-hsbc-and-standard-chartered-accused-of-links-to-iran-financial-crime-activity/
- https://www.occrp.org/en/investigation/the-cat-and-the-stock-footage-ceo-how-a-digital-trail-helped-unmask-an-iranian-money-machine
- https://www.transparency.org.uk/news/londons-role-irans-financial-networks-and-why-it-matters-now
- https://www.nytimes.com/2026/03/11/nyregion/halkbank-turkey-sanctions-money-laundering.html
- https://nationalinterest.org/blog/middle-east-watch/how-irans-leaders-hide-their-billions
- https://scantv.al/english/lajme/bota/kontroll-skemave-iraniane-te-pastrimit-te-parave-thesari-amerikan-u-k-i31250
- https://www.telegraph.co.uk/news/2026/04/18/banking-giants-accused-links-iran-money-laundering/
- https://www.kurdistan24.net/en/story/901932/uae-dismantles-hezbollah-and-iran-linked-network-involved-in-money-laundering-and-terror-financing
- https://www.nytimes.com/2026/02/23/technology/binance-employees-iran-firings.html
- https://theijf.org/brief/iran-crypto-laundering-in-canada
- https://www.bloomberg.com/news/articles/2026-02-26/us-says-swiss-bank-mbaer-could-lose-access-to-financial-system
- https://www.telegraph.co.uk/news/2026/03/07/two-british-companies-linked-iran-billionaire-shadow-banker/
- https://www.wsj.com/finance/currencies/binance-iran-sanctions-financing-staff-b1648133
- https://iranfocus.com/economy/56492-iran-north-korea-financial-links-revealed-in-money-laundering-network/
- https://www.thestar.com/news/investigations/suspicious-transactions-at-gta-crypto-shops-reveal-alleged-links-to-iran-backed-terror-groups-is/article_a18562a4-1cc8-47e9-a2fc-b20b01a01e1e.html
- https://fincrimecentral.com/fincen-iran-shadow-banking-money-laundering/
- https://www.iranintl.com/en/202504029505
- https://iran-hrm.com/2025/09/04/irans-fake-charities-corruption-money-laundering-and-manufactured-poverty/
- https://www.iranintl.com/en/202307074269
- https://nordicmonitor.com/2023/05/erdogan-government-warns-convicted-banker-to-keep-quiet-about-new-money-laundering-claims-related-to-iran/
- https://www.fdd.org/analysis/2025/02/24/a-high-risk-jurisdiction-fatf-keeps-iran-on-blacklist-calls-for-countermeasures/
- https://www.amlintelligence.com/2024/02/news-the-small-hamburg-bank-at-centre-of-iran-money-laundering-claims-and-probe-by-bafin/
- https://www.iranintl.com/en/202204100227
- https://www.atlanticcouncil.org/blogs/econographics/global-sanctions-dashboard-how-iran-evades-sanctions-and-finances-terrorist-organizations-like-hamas/
- https://www.spiegel.de/international/business/circumventing-u-s-sanctions-turkish-state-owned-bank-suspected-of-transferring-usd1-5-billion-to-tehran-a-c7e76706-0900-442d-bfd5-c95a9d26a055
- https://www.iranintl.com/en/202305098088
- https://www.kurdistan24.net/en/story/868495/washington-cracks-down-on-iran-linked-money-laundering-and-arms-smuggling-in-iraq
- https://www.arabnews.com/node/1533851/middle-east
- https://www.politico.eu/article/hamburg-bank-suspected-as-financial-hub-for-iranian-terror/
- https://www.arabnews.com/node/1725436/business-economy
- https://www.arabnews.com/node/1627236/amp

- https://en.radiofarda.com/a/canada-arrests-seven-iranians-for-money-laundering/29769999.html
- https://www.occrp.org/en/news/slovenia-opens-investigation-into-iran-related-money-laundering-scandal
- https://iranwire.com/en/features/68458/
- https://www.acfcs.org/unraveling-a-complex-web-a-primer-on-hamas-funding-sources-iranian-support-global-connections-and-compliance-concerns-considerations
- https://gfintegrity.org/press-release/anti-money-laundering-crackdown-contributed-collapse-iranian-currency/
- https://www.kharon.com/brief/illicit-iran-trading-network-charged-in-u-s-tied-to-vast-money-laundering-network-global-petrochemical-commerce
- https://www.arabnews.com/node/1160786/amp
- https://www.occrp.org/en/feature/the-man-that-got-away-iranian-fugitive-named-in-canadian-espionage-case
- https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-maduro-hezbollah-nexus-how-iran-backed-networks-prop-up-the-venezuelan-regime/
- https://www.aljazeera.com/economy/2012/12/11/hsbc-to-pay-1-9bn-money-laundering-fine
- https://www.abc.net.au/news/2012-08-08/standard-chartered-shares-plunge-after-money-laundering-claim/4184294
- https://www.transparency.org.uk/news/londons-role-irans-financial-networks-and-why-it-matters-now
- https://www.arabnews.com/node/2643499/amp
- https://cryptobriefing.com/uk-sanctions-iran-linked-entities/
- https://www.iranintl.com/en/202602279443
- https://www.msn.com/en-us/news/insight/iran-s-criminal-networks-undermine-us-sanctions-strategy/gm-GMCB6597CC?gemSnapshotKey=GMCB6597CC-snapshot-1&uxmode=ruby

- https://icct.nl/publication/hybrid-threat-signals-assessing-possible-iranian-involvement-recent-attacks-europe
- https://www.algemeiner.com/2026/05/29/irans-global-terror-network-sparks-growing-alarm-west/
- https://globalinitiative.net/analysis/iran-pressure-us-gunboat-diplomacy-sanctions-evasion-corruption/
- https://www.meforum.org/mef-observer/irans-mafia-hit-squads-and-tehrans-hybrid-war-on-the-wests-streets
- https://www.fdd.org/analysis/2026/03/13/irans-war-across-europe-complacency-must-finally-end/
- https://www.thenationalnews.com/news/uk/2026/03/24/iran-builds-european-terror-network-to-attack-jewish-targets/
- https://www.iranintl.com/en/202602247024
- https://www.thenationalnews.com/news/europe/2025/12/25/irans-foxtrot-sanctuary-for-crime-boss-angers-critics-of-silent-sweden/
- https://www.channelstv.com/2026/04/08/five-minors-tried-in-sweden-over-iran-dissident-murder-plot/
- https://asiacrimecentury.substack.com/p/irans-covert-war-in-the-uk-state
- https://www.meforum.org/mef-observer/irans-cartel-axis-on-americas-doorstep
- https://www.meforum.org/mef-observer/iran-built-a-cocaine-drone-corridor-in-bolivia-washington-looked-away
- https://www.meforum.org/mef-observer/irans-terror-pipeline-at-americas-border
- https://www.jpost.com/middle-east/iran-news/article-892251
- https://icct.nl/publication/iranian-external-operations-europe-criminal-connection

- https://www.thenationalnews.com/news/2025/12/23/sweden-kurdish-gang-foxtrot-crime/
- https://www.thebureau.news/p/irans-long-arm-sleeper-cells-criminal
- https://nationalpost.com/opinion/canada-can-no-longer-ignore-irans-dangerous-shadow-network
- https://www.longwarjournal.org/archives/2025/03/irans-ties-to-western-organized-crime-networks.php
- https://holliesmckay.substack.com/p/why-us-officials-are-scrambling-to
- https://globalinitiative.net/analysis/irans-criminal-statecraft-how-teheran-weaponizes-illicit-markets/
- https://www.gov.uk/government/news/uk-sanctions-iranian-organised-crime-network
- https://thesoufancenter.org/intelbrief-2024-november-1/
- https://www.reuters.com/world/uk/uk-adds-two-new-designations-its-iran-sanctions-list-2025-04-14/
- https://www.jpost.com/international/islamic-terrorism/article-867803
- https://smallwarsjournal.com/2025/05/29/iran-using-criminal-gangs-for-hit-jobs-abroad-court-papers-show-bbc/
- https://www.iranintl.com/en/202504229418
- https://www.iranintl.com/en/202506197511
- https://www.atlanticcouncil.org/blogs/menasource/the-case-for-designating-iran-linked-crime-networks-as-ftos/
- https://www.thecipherbrief.com/tehrans-espionage-network-in-the-u-s-is-bigger-and-bolder-than-you-think
- https://www.jns.org/israel-news/sweden-exposes-irans-europe-wide-israeli-assassination-network
- https://ctc.westpoint.edu/tehrans-homeland-option-terror-pathways-for-iran-to-strike-in-the-united-states/
- https://www.fdd.org/analysis/2025/03/14/u-s-levies-sanctions-against-swedish-foxtrot-gang-with-ties-to-iran/
- https://www.iranintl.com/en/202504248101
- https://www.timesofisrael.com/mossad-iran-backed-criminal-networks-behind-attacks-on-israeli-embassies-in-europe/
- https://www.cnn.com/interactive/2025/world/iran-israel-swedish-teenagers-shadow-war-intl-invs
- https://www.jpost.com/international/article-865360
- https://www.washingtonpost.com/world/2024/09/12/iran-criminal-gangs-target-dissidents/
- https://www.israelnationalnews.com/news/410724
- https://www.voanews.com/a/report-iran-increases-ties-with-criminal-networks-to-attack-critics-in-us-europe-/7781915.html
- https://www.fdd.org/analysis/2025/03/21/two-mobsters-found-guilty-of-plotting-to-assassinate-iranian-american-journalist-masih-alinejad/
- https://www.thetimes.com/world/europe/article/iran-mafia-assassinations-europe-sg2k833v9
- https://www.iranintl.com/en/202409056555
- https://www.ncr-iran.org/en/news/terrorism-a-fundamentalism/irans-regime-and-its-strategic-outsourcing-to-criminal-gangs-worldwide/
- https://ctc.westpoint.edu/hezbollahs-procurement-channels-leveraging-criminal-networks-partnering-iran/
- https://research.checkpoint.com/2026/iranian-mois-actors-the-cyber-crime-connection/
- https://www.halcyon.ai/ransomware-alerts/iranian-use-of-cybercriminal-tactics-in-destructive-cyber-attacks-2026-updates
- https://industrialcyber.co/reports/iranian-state-sponsored-hackers-exploit-microsoft-exchange-fortinet-flaws-to-access-us-infrastructure-networks-crs-finds/

- https://www.kelacyber.com/blog/beyond-the-regime-how-iran-weaponizes-cybercrime-and-ransomware-tactics/
- https://www.cybersecuritydive.com/news/iran-threat-group-false-flag-social-engineering/819454/
- https://www.jpost.com/defense-and-tech/article-895078
- https://securityaffairs.com/191765/breaking-news/iranian-cyber-espionage-disguised-as-a-chaos-ransomware-attack.html
- https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/
- https://www.lawfaremedia.org/article/successful-war-leaves-iran-with-one-option--cyber
- https://www.foxnews.com/opinion/irans-cyberwar-targets-ordinary-americans-we-need-dismantle-hacker-network
- https://www.csoonline.com/article/4167985/iranian-state-backed-spies-pose-as-ransomware-slingers-in-false-flag-attacks.html
- https://www.timesofisrael.com/defense-officials-say-hundreds-of-iranian-cyberattacks-foiled-in-past-months/
- https://www.thenationalnews.com/future/technology/2026/04/10/iranian-cyber-attacks-move-from-disruptive-to-complex-threats-in-gulf/
- https://www.theregister.com/security/2026/03/02/irans-cyberwar-has-begun/4660301
- https://www.halcyon.ai/ransomware-research-reports/pay2key-iranian-linked-ransomware-is-back-back-again
- https://industrialcyber.co/ransomware/iranian-hackers-target-us-critical-infrastructure-through-ransomware-proxies-kela-warns/
- https://www.abc.net.au/news/2026-03-13/iran-cyber-attack-stryker-hospitals/106452066
- https://www.theregister.com/security/2026/03/10/cybercrime-isnt-just-a-cover-for-irans-government-goons/5226388
- https://www.theregister.com/security/2026/05/01/pro-iran-group-turns-ubuntu-ddos-into-shakedown/5224575
- https://www.govtech.com/blogs/lohrmann-on-cybersecurity/new-federal-strategies-rising-risk-from-iran-top-cyber-themes
- https://www.theregister.com/security/2026/03/05/iran-intelligence-backdoored-us-bank-airport-networks/5041702
- https://www.theregister.com/security/2026/03/02/businesses-told-to-harden-defenses-amid-iran-conflict-risk/4838891
- https://www.theregister.com/security/2026/03/31/iran-targets-m365-accounts-with-password-spraying-attacks/5229934
- https://www.theregister.com/security/2026/03/19/microsoft-intune-lock-it-down-warn-feds-after-stryker/5221832
- https://www.darkreading.com/threat-intelligence/iran-mois-criminals-cyberattacks
- https://industrialcyber.co/critical-infrastructure/ncsc-warns-of-cyber-spillover-risk-amid-middle-east-conflict-as-experts-flag-potential-iranian-attacks-on-critical-infrastructure/
- https://www.govtech.com/security/feds-warn-against-lone-wolf-cyber-attacks-amid-iran-conflict
- https://cybermagazine.com/news/iran-war-cyber-and-kinetic-warfare-converge
- https://securityaffairs.com/189069/cyber-warfare-2/iran-linked-hackers-target-ip-cameras-across-israel-and-gulf-states-for-military-intelligence.html
- https://securityaffairs.com/189865/cyber-warfare-2/pro-iranian-nasir-security-is-targeting-energy-companies-in-the-gulf.html
- https://financialpost.com/financial-times/irans-hackers-go-to-war
- https://www.thenews.com.pk/latest/1399155-iranian-cyberattacks-surge-8x-across-middle-east
- https://www.mercurynews.com/2026/04/08/pro-iran-group-takes-credit-for-cyberattacks-on-chime-pinterest/

- https://abcnews4.com/news/nation-world/doj-moves-to-disrupt-iran-linked-cyber-network-as-security-concerns-grow-washington-tehran-google-sleeper-cells-united-states
- https://the420.in/iran-cyber-war-strategy-us-israel-proxy-hackers-ai-analysis/
- https://www.ketv.com/article/ncite-warns-of-iranian-based-cyber-attacks-in-nebraska/70669401
- https://www.scworld.com/brief/u-s-offers-10-million-reward-for-iranian-cyber-suspects
- https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4229506/nsa-cisa-fbi-and-dc3-warn-iranian-cyber-actors-may-target-vulnerable-us-network/
- https://www.thesun.co.uk/news/38396300/iranian-hackers-chaos-uk-basij-militia/
- https://www.meforum.org/mef-observer/x-uncovers-irans-cyber-army-efforts-to-manipulate-british-public-opinion
- https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3935330/iranian-cyber-actors-access-critical-infrastructure-networks/
- https://www.fbi.gov/news/stories/iran-at-center-of-cyber-crime-charges-in-three-cases-091820
- https://www.securitymagazine.com/articles/101737-iranian-cyber-actors-may-target-entities-of-interest-in-us-warns-cisa
- https://hackread.com/iranian-hackers-fake-job-breach-europe-industries/
- https://www.securityweek.com/iranian-hackers-preferred-ics-targets-left-open-amid-fresh-us-attack-warning/
- https://www.meritalk.com/articles/cisa-warns-of-iranian-attacks-against-us-dib-networks/
- https://www.theregister.com/security/2025/07/21/4-new-android-spyware-samples-linked-to-irans-intel-agency/1550706
- https://www.bbc.com/news/articles/c0lw0081e1yo
- https://www.thenationalnews.com/news/europe/2025/04/24/german-politician-falls-victim-to-iranian-hackers-posing-as-expert-on-hezbollah/
- https://www.bbc.com/news/world-europe-62821757
- https://www.nationalcrimeagency.gov.uk/news/iranian-who-ran-payment-platform-for-cyber-criminals-arrested-in-uk
- https://www.iranintl.com/en/202403142380
- https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector
- https://securityaffairs.com/167730/apt/apt33-used-new-tickler-malware.html
- https://www.cnbc.com/2024/06/26/americas-drinking-water-under-attack-china-russia-and-iran.html
- https://industrialcyber.co/cisa/iranian-hackers-use-brute-force-credential-access-activity-to-target-critical-infrastructure-organizations/
- https://www.theregister.com/security/2023/02/04/microsoft-blames-iran-backed-crew-for-charlie-hebdo-breach/652470
- https://www.theregister.com/security/2024/08/19/openai-kills-iranian-accounts-spreading-us-election-disinfo/1252442
- https://www.darkreading.com/vulnerabilities-threats/iran-cyber-centers-dodge-sanctions-sell-cyber-operations
- https://thehackernews.com/2023/08/iranian-company-cloudzy-accused-of.html
- https://securityaffairs.com/24923/cyber-crime/ajax-security-team-iran.html
- https://the420.in/los-angeles-transit-cyberattack-iranian-link/
- https://cyberpress.org/iranian-actors-join-criminal-nexus/
- https://the420.in/kash-patel-fbi-email-hack-handala-iran-cyberattack-leak/
- https://the420.in/us-iran-cyber-warfare-operation-epic-fury-strategy/
- https://the420.in/iran-hackers-stryker-cork-cyberattack-2026-wiper-malware/
- https://icct.nl/publication/tehran-europe-terrorism-risks-after-killing-irans-ayatollah

- https://www.visionofhumanity.org/how-the-iran-conflict-could-drive-a-new-wave-of-terrorism-in-the-west/
- https://www.euractiv.com/news/exclusive-eu-terrorism-threat-heightened-due-to-iran-europol-says/
- https://theconversation.com/the-iranian-revolution-transformed-global-extremism-replacing-left-wing-radicalism-with-religion-272444
- https://www.aa.com.tr/en/europe/french-court-jails-iranian-woman-for-justifying-terrorism/3841789
- https://icct.nl/publication/hybrid-threat-signals-assessing-possible-iranian-involvement-recent-attacks-europe
- https://www.dowjones.com/business-intelligence/blog/europe-north-america-terrorism-threat-elevated-iran-conflict/
- https://www.atalayar.com/en/articulo/reports/threat-of-iranian-linked-shia-terrorism-in-europe/20260305100000223791.html
- https://www.cnn.com/2026/03/14/us/video/cnn-newsroom-whitfield-cynthia-miller-idriss-michigan-terror-attack-old-dominion-terrorism
- https://www.visionofhumanity.org/global-terrorism-falls-to-a-decade-low-but-western-fatalities-surge/
- https://time.com/article/2026/03/13/iran-war-us-attacks-threat-cyberattacks-drones-terrorism-proxies/
- https://www.theguardian.com/world/2026/mar/27/golders-green-ambulances-firebomb-iran-involvement-terror-campaigns
- https://www.isdglobal.org/digital-dispatch/a-resurgent-and-diversifying-threat-islamist-extremist-violence-in-germany-in-the-wake-of-october-7-2/
- https://www.lemonde.fr/en/international/article/2026/03/25/belgium-s-pro-iranian-cells-aimed-to-demonstrate-their-capacity-to-act-by-attacking-jewish-sites_6751789_4.html
- https://www.npr.org/2026/03/19/nx-s1-5752332/iran-war-terrorism-threat-us
- https://www.theguardian.com/uk-news/2026/apr/23/iran-low-level-hybrid-warfare-arson-attacks-uk-europe
- https://www.meforum.org/mef-observer/is-iran-radicalizing-indian-shia
- https://www.nytimes.com/2026/03/14/us/iran-us-attacks-terrorism-michigan-old-dominion.html
- https://www.straitstimes.com/opinion/singapore-must-stay-vigilant-for-spillover-security-risks-from-iran-war
- https://www.channelnewsasia.com/shorts/singapore-steps-up-security-checkpoints-terrorism-threats-rise-amid-iran-war-shanmugam-6054016
- https://www.jpost.com/international/article-889005
- https://ec.europa.eu/newsroom/home/items/895036/en
- https://www.amny.com/news/murder-for-hire-plot-at-center-of-brooklyn-terrorism-trial-over-alleged-scheme-to-kill-trump/
- https://telanganatoday.com/indian-agencies-flag-online-radicalisation-push-amid-israel-us-iran-conflict
- https://www.jpost.com/diaspora/article-864226
- https://www.politico.eu/article/uk-police-arrest-terror-probe-iran-terrorism-investigations/
- https://www.theguardian.com/uk-news/2025/may/04/uk-arrests-five-men-including-four-iranians-over-suspected-terrorist-plot
- https://aijac.org.au/fresh-air/malaysias-role-in-supporting-irans-terrorism/
- https://www.aljazeera.com/news/2024/7/24/germany-bans-muslim-group-citing-extremism-ties-to-iran-and-hezbollah
- https://www.thefp.com/p/ayaan-hirsi-ali-iran-is-collapsing

- https://www.al-monitor.com/originals/2026/01/iranian-parliament-warns-jihad-if-supreme-leader-attacked-isna
- https://www.iranintl.com/en/202202088610
- https://institute.global/insights/geopolitics-and-security/beyond-borders-expansionist-ideology-irans-islamic-revolutionary-guard-corps
- https://www.jpost.com/international/article-720003
- https://jcfa.org/from-the-west-bank-to-u-s-campuses-irans-psychological-influence-is-spreading/
- https://www.fdd.org/analysis/2024/07/10/iran-supporting-and-funding-pro-hamas-protests-in-the-u-s/
- https://www.theatlantic.com/international/archive/2025/06/iran-propaganda-palestine/683322/
- https://abcnews.com/Politics/iranian-government-actors-seeking-advantage-pro-palestinian-protests/story?id=111786372
- https://www.jns.org/u.s.-news/iran-funding-anti-israel-protests-us-intelligence-chief-says
- https://jinsa.org/iran-finances-u-s-campus-protests-top-intel-official/
- https://apnews.com/article/gaza-war-protests-iran-foreign-influence-95e0a161119ed0e060332feda95b4e4f
- https://www.theguardian.com/world/2025/jun/24/uk-protest-group-palestine-action-denies-iran-funding-faces-ban-home-office
- https://www.iranintl.com/en/202311038402
- https://www.iranintl.com/en/202408012272
- https://www.jpost.com/middle-east/article-888705
- https://www.thetimes.com/world/middle-east/article/what-is-irgc-iran-revolutionary-guard-fbcmfhqfz
- https://www.iranintl.com/en/202511273508
- https://www.iranintl.com/en/202511238766
- https://www.iranintl.com/en/202509081757
- https://iranwire.com/en/news/143782-iran-reports-rising-drug-addiction-declining-purity-of-narcotics/
- https://www.bbc.com/news/world-middle-east-40397727
- https://www.iranintl.com/en/202408126589
- https://www.iranintl.com/en/202507064479
- https://thearabweekly.com/houthi-drug-trade-fuels-instability-yemen-and-middle-east-iran-role-suspected
- https://jcfa.org/iran-spreads-illegal-drugs-in-the-middle-east-western-hemisphere-and-the-far-east/
- https://armenpress.am/en/article/1235720
- https://www.jns.org/israel-news/iran-hezbollah-implicated-in-irelands-largest-drug-bust
- https://globalinitiative.net/analysis/under-the-shadow-illicit-economies-in-iran/
- https://globalinitiative.net/analysis/iran-meth-ephedra-plant-afghanistan-ephedrine/
- https://www.thejournal.ie/drugs-seamus-boland-links-to-iran-and-kinahan-6794992-Aug2025/
- https://thearabweekly.com/jordan-wages-border-drugs-war-against-iran-backed-groups-syria
- https://www.middleeastmonitor.com/20200429-study-drugs-kill-4000-people-annually-in-iran/
- https://www.voanews.com/a/bulgaria-seizes-288-kilos-of-heroin-in-truck-from-iran-/4881852.html
- https://en.majalla.com/node/229121/opiniondrugs-iran-has-new-artillery
- https://www.scmp.com/week-asia/politics/article/3306226/irans-meth-cartels-target-australia-malaysias-port-klang
- https://www.voanews.com/a/italian-police-make-major-heroin-haul-on-ship-from-iran/4650157.html
- https://www.arabnews.com/node/1716966

- https://www.aljazeera.com/news/2021/10/12/india-adani-ports-cargo-afghanistan-pakistan-iran-heroin-gujarat
- https://www.longwarjournal.org/archives/2024/06/jordanian-authorities-thwart-major-drug-smuggling-operation-linked-to-iran-backed-militias.php
- https://www.ynetnews.com/article/bysz8kuwn
- https://en.radiofarda.com/a/iran-drug-addiction-campaign-failed/29216824.html
- https://www.rferl.org/a/us_says_iran_general_key_to_afghan_drug_trade/24508321.html
- https://www.ncr-iran.org/en/news/terrorism-a-fundamentalism/iran-news-jordan-intensifies-border-operations-against-iranian-linked-drug-smuggling-networks/
- https://english.alarabiya.net/features/2018/08/16/How-the-Iranian-regime-allows-drug-trafficking-for-foreign-currency-liquidity-