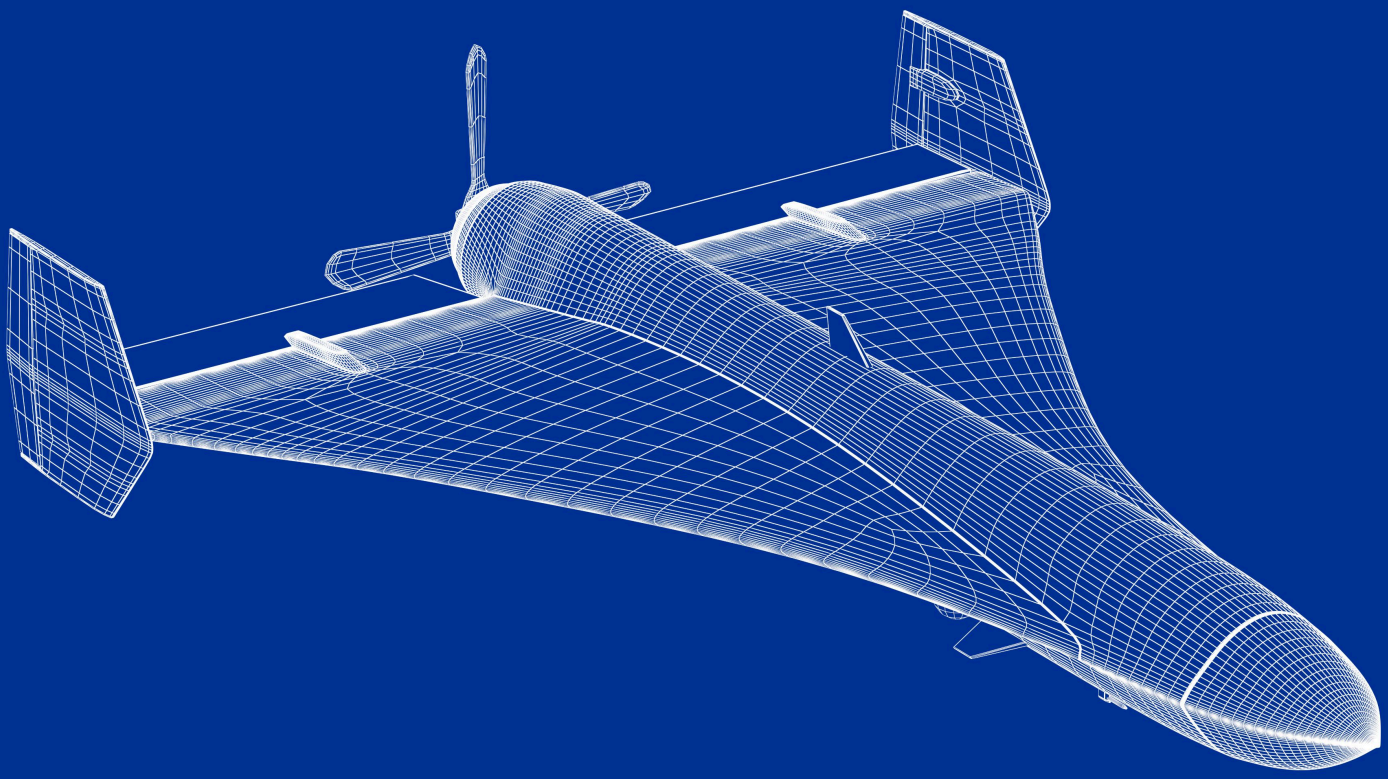
STRIDER

REPORT

IRAN'S DRONE PROGRAM

How The Islamic Republic Exploited Commercial Supply Chains to Reshape Modern Warfare



Executive Summary

With its drone program, Iran has demonstrated how a sanctioned state can reshape modern warfare through the systematic exploitation of global commercial supply chains. Despite comprehensive international sanctions, Tehran continues to produce and export drone systems actively reshaping evolving conflicts, including in Ukraine and across the Middle East.

Introduction

As conflict escalates across the Middle East and the war in Ukraine grinds into its fourth year, one weapon system has emerged at the center of both: Iran's Shahed drone. Cheap, mass-produced, and increasingly lethal, the Shahed has become the signature munition of a new era of asymmetric warfare.

Iran's drone program has become one of the Islamic Republic's most effective military tools, allowing Tehran to project power far beyond its borders while offsetting conventional military disadvantages. **Through the development and mass production of the Shahed drone, Iran has changed the landscape of modern warfare—first through its export of drones to Russia for use in Ukraine, and now through the direct deployment of Shaheds in conflicts with Israel and the United States.**

Even under sweeping international sanctions, Iran sustains its drone production through a global network of front companies and commercial intermediaries procuring dual-use foreign components. Understanding how that network operates—and who enables it—starts with the history of the program itself.

Key Takeaways

The Shahed-136 loitering munition has become the signature system of Iran's drone arsenal and has been deployed in Ukraine (as Russia's Geran-2), against Israel and Saudi Arabia, and against other targets on behalf of proxies.

Iran's ability to circumvent sanctions via dual-use commercial components and front companies has sustained its drone production despite international pressure. Recovered Shaheds have yielded Chinese and Austrian engines and Western microelectronics.

Pars Aero Institute Kerman—an Iranian drone supplier with documented ties to the Islamic Republic's military—and its Hong Kong and People's Republic of China (PRC) suppliers remain unsanctioned despite connections to Iranian military production and PLA-connected networks.

The Rise of Iran's Drone Program

Iran's drone program emerged from a strategic calculation: by leveraging an asymmetric warfare doctrine, Tehran could offset conventional disadvantages against technologically superior adversaries. **Drones would enable Iran to project power at long range without exposing conventional forces, to saturate air defenses through swarm tactics, and to arm proxies and partners with low-cost, mass-producible systems.**

The doctrine was put on display in October 2016 when the Islamic Revolutionary Guard Corps (IRGC) conducted the first drone swarm use against ISIS in Syria. Since then, Iran has aggressively refined its program, built it out at scale, and established itself as a global drone superpower. As of January 2026, the Iranian Army had integrated 1,000 "strategic" drones across its service branches and the IRGC maintains a secretive offensive drone unit responsible for maritime and multi-domain strikes.

The December 2011 downing of a U.S. RQ-170 Sentinel reconnaissance drone largely intact by Iran's cyberwarfare proved a pivotal moment for the drone program. Today, Iran operates at least six Shahed variants derived from reverse engineering of the captured RQ-170. That includes its signature system, the Shahed-136. Dubbed the "Kalashnikov of drones" as a nod to the Soviet rifle's reputation for its low cost and ease of mass production, it has an estimated range of 2,000–2,500 km, a 40–50 kg warhead, and GPS-guided navigation designed to fly at low altitude to evade radar. The Shahed-136 has been deployed in Ukraine, in Iran's April 2024 mass attack on Israel, and in Houthi strikes against Saudi Arabia.

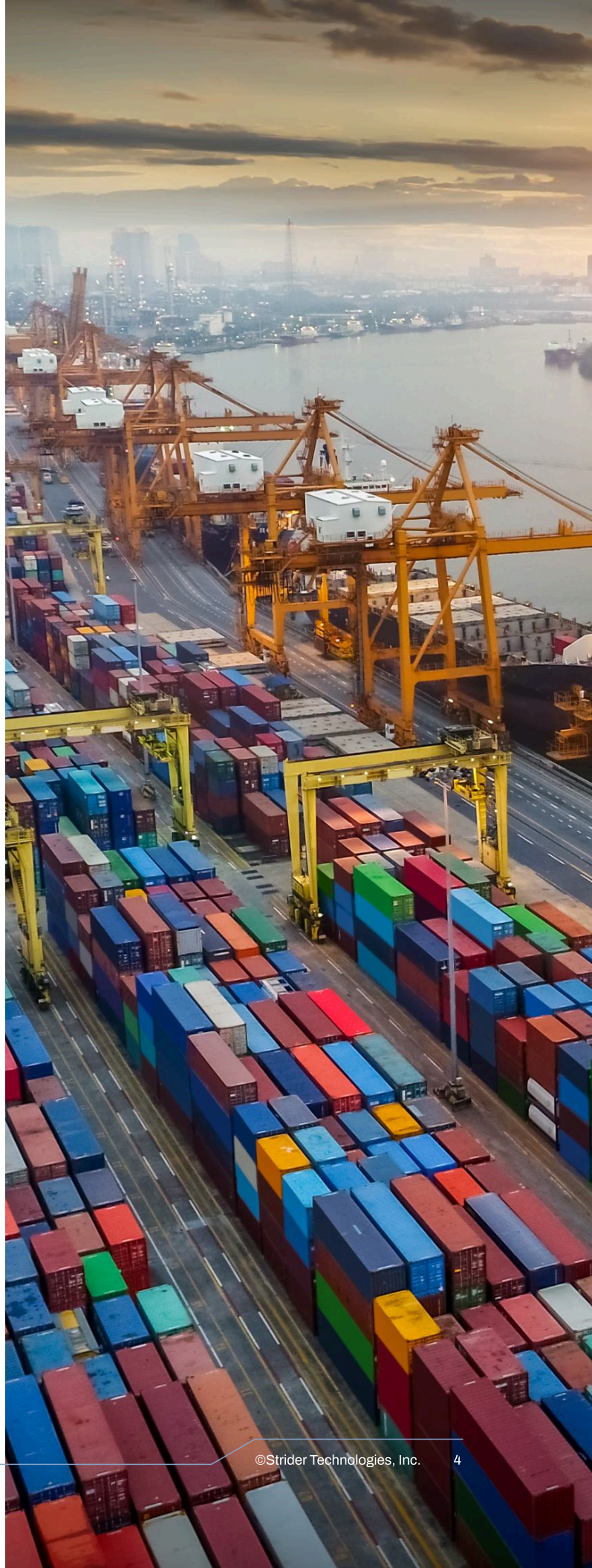
The program's impact extends well beyond Iranian territory. Drone technology has proliferated to Russia, where the Shahed-136 flies as the Geran-2 and is now in licensed production at Yelabuga, as well as to Hezbollah (~2,000 drones), Houthi forces, and Iraqi militias conducting attacks on U.S. facilities. Since early March 2026, coordinated multi-front campaigns have struck U.S. and Israeli targets simultaneously from Yemen, Iraq, Lebanon, and Syria.

Foreign Components Discovered Inside Iranian Drones

When Ukrainian forces began shooting down Russian-deployed Shaheds in the fall of 2022, what they found inside the wreckage was unexpected. **Forensic analysis of captured and recovered Shaheds identified Chinese and Austrian engines and Western microelectronics, including Swedish and U.S. high-technology components.**

That evidence points to a broader pattern: domestic advances (such as the Jahesh-700 engine and stealth platforms) have reduced, but not eliminated, Iran's dependence on foreign supply chains. Iran has sought to diversify its production base to reduce dependence on any single source or supplier that can be easily targeted via sanctions. Iranian drone production has also adapted to rely heavily on available commercial parts—dual-use electronics and hardware sourced from multiple countries, moving through global trade channels with minimal scrutiny. For example, a South Korean servomotor recovered from a Houthi drone in Yemen was traced back to a Tehran toy shop that sold remote-controlled aircraft. This reliance on the global commercial supply chain has become one of the program's most durable strengths.

However, the mere presence of these components in Iranian drones does not necessarily implicate their makers. Many companies whose components have been discovered in Iranian drones have reinforced their compliance with the law and condemned any unauthorized use. Many have strict internal compliance policies and programs in place and many direct their customers and distributors to follow similar rules. **But the networks moving these components operate in the gaps between what compliance programs cover and what enforcement can see. The diversion happens downstream—through intermediaries, front companies, and transshipment hubs that exist to obscure the components' final destination.**



The Procurement Network

The path from a foreign manufacturer to an Iranian assembly line runs through a deliberately constructed network. In a submission to G7 governments in 2023, Ukraine identified the primary transshipment corridor for these components as Turkey, India, Kazakhstan, Uzbekistan, Vietnam, and Costa Rica, with the UAE also emerging as a particularly significant re-export hub. Components move through this corridor via front companies and commercial channels designed to obfuscate their origin and end use.

For example, a UN probe discovered that Swedish high-technology components were shipped to Iran via an Indian food-trading front company. Those components were then assembled into drones that were used to strike oil facilities in Saudi Arabia in May and September 2019, after which they were retrieved and analyzed. **The mix of domestic assembly and foreign sourcing helps Iran sustain production, replace restricted parts, and scale exports to partners and proxies despite sanctions pressure**.

People's Republic of China (PRC) and Hong Kong intermediaries, in particular, have become increasingly important for Iranian manufacturers and procurement networks to source engines, electronics, and other subcomponents as Iran becomes more cut off from the global economy. In February 2025, the U.S. Treasury sanctioned six PRC- and Hong Kong-based entities for procuring drone parts for Iranian firms linked to drone and missile production, calling out a pattern of third-country sourcing on behalf of Iran's military-industrial base. But the broader procurement apparatus remains intact.

Case Study: Pars Aero

Strider research has uncovered one such intermediary, and its suppliers, that are enabling Iran's drone program. Pars Aero Institute Kerman (Pars Aero) is an Iranian drone company that has supplied "spy" drones to the Islamic Republic of Iran Army. Strider researchers discovered a 2020 letter sent to the CEO of Pars Aero from a member of the Islamic Republic of Iran Army Aviation thanking him for Pars Aero's assistance constructing the Azar identification UAV and for serving the Iran Aviation Industries Organization. Iran Aviation Industries was sanctioned by the United States in 2013 for being owned or controlled by the Ministry of Defense and Armed Forces Logistics.

Pars Aero is a "dealer" of Hong Kong-based Foxtech Hobby Co. Ltd. and sources its supplies of XAG and DJI drones from Hong Kong and Foxtech's mainland PRC counterpart, Huixinghai Technology (Tianjin) Co. Ltd. Foxtech claims it does not sell drones to Iran, yet a 2020 authorization letter from Foxtech to Pars Aero reveals that the company was aware of Pars Aero's Kerman, Iran address. Additionally, videos from a Pars Aero-led UAV pilot training held in Yazd, Iran in June 2025 show an IRGC officer in attendance and participating in the ribbon cutting ceremony.

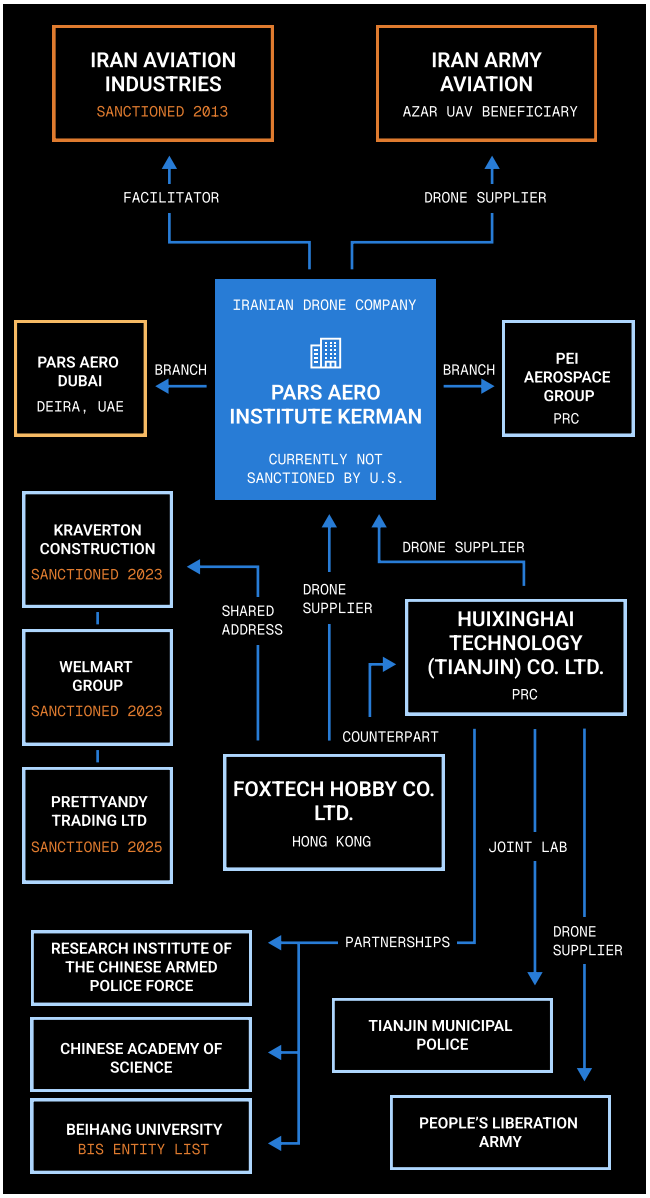
Strider research uncovered product images posted by Huixinghai Technology (Tianjin) Co. Ltd., still live as of mid-March 2026, that show a drone bearing resemblance to a Shahed. Huixinghai has also received a letter of appreciation from Unit 63629 of the People's Liberation Army (PLA) for the company's cooperation in supplying the PRC military with drones. The company has also partnered with the Research Institute of the Chinese Armed Police Force, the Chinese Academy of Science, and Beijing University of Aeronautics and Astronautics (now known as Beihang University). A Seven Sons of National Defense university, Beihang University is on the BIS Entity List due to its involvement in PRC military rocket and UAV systems. Additionally, Huixinghai Technology (Tianjin) Co. Ltd. operates a joint lab with the Tianjin Municipal Police.

Foxtech Hobby Co. Ltd.'s Hong Kong address is shared by several companies, three of which were sanctioned by the U.S. Two of the companies, Kraverton Construction and Development Limited and Welmart Group Limited, were sanctioned by the United States in 2023 for acting as shell companies "with suspected links to Russian organized crime and money laundering."

The third company, Prettyandy Trading Ltd., was also sanctioned by the U.S. in June 2025 for “facilitating international transactions on behalf of Iranian entities.”

In addition to the Foxtech ecosystem, Pars Aero also operates branches in Deira, Dubai, as well as its own company in the PRC under the name PEI Aerospace Group. This further illustrates their dependence on imported drone components to supplement their manufacturing capability inside Iran.

As of March 12, 2026, Pars Aero, Foxtech Hobby Co. Ltd., and Huixinghai Technology (Tianjin) Co. Ltd. were not found on any U.S. or allied sanctioned lists.



Mapping Supply Chain Risk

Nearly all of Iran's primary drone manufacturers—Shahed Aviation Industries, Qods Aviation Industries, and HESA—have been sanctioned by numerous countries. **But Iran's ability to circumvent sanctions via dual-use commercial components and front companies has sustained its drone production despite international pressure.**

This illustrates the importance of supply chain due diligence. Even with compliance to existing sanctions, end-to-end supply chain due diligence requires full visibility—who distributors sell to, who shares addresses with partners, and whether those partners have ties to sanctioned programs or state-linked military procurement networks. The Pars Aero case demonstrates how ordinary commercial trade can blur into support for a sanctioned military-industrial base: PRC and Hong Kong suppliers provide engines, electronics, and drone platforms, while Iranian firms with documented military ties integrate them into the defense supply chain. Even where foreign companies disclaim sales to Iran, distributor relationships, third-country branches, and parallel procurement channels can still enable onward transfer.

Organizations that rely on sanctions designations alone to manage supply chain risk are leaving themselves exposed to legal liability, reputational damage, and the possibility of finding their products in the next weapons system traced back to Iran.

Conclusion

What the Shahed program reveals, above all, is how systematically Iran has learned to exploit the global commercial supply chain and how far that exploitation has carried it despite comprehensive international sanctions.

As this report illustrates, unsanctioned commercial entities can sit at the heart of a sanctioned military procurement architecture. At the time of this report's publication, Pars Aero, Foxtech Hobby Co. Ltd., and Huixinghai Technology (Tianjin) Co. Ltd. were not found on any U.S. or allied sanctioned lists despite evidence that shows direct connections to Iran's drone program.

While strict adherence to sanctions is important, it is often insufficient to keep up with the evolving tactics of adversarial nation-states. Organizations should consider sanctions compliance the floor, not the ceiling, when evaluating partners in their supply chains.

Strider's strategic intelligence helps organizations map the entities, individuals, and relationships connecting commercial supply chains to sanctioned or high-risk end users. By identifying distributor networks and intermediary firms, as well as revealing potential connections to adversarial nation-states, Strider enables organizations to screen high-risk partners before exposure occurs.

As new conflicts arise and escalate across multiple fronts, new actors will be designated, new networks exposed, and new compliance requirements imposed. For organizations seeking to stay ahead of the curve, leveraging strategic intelligence to monitor supply chains, partner relationships, and potential ties to adversarial nation-states remains essential.

For sourcing information or more insight into information detailed in this report and Strider's tools, reach out to our team via email at info@striderintel.com.