THREAT ANALYSIS

IRAN

Recorded Future®

By Insikt Group®

August 1, 2024

Production and Proliferation: The Risks of the Burgeoning Iranian Drone Industry

Iran's growing drone industry poses major challenges to global businesses and Western governments – beyond the well-known physical security threat. Tehran's procurement network is steadily evolving.

Insikt Group identified five major risks related to compliance, reputation, technology transfer, proliferation, and cybersecurity, using case studies to portray the scope of Iran's illicit activity.

Corporations and Western governments can help mitigate these risks through compliance programs, intelligence collection, and an upgraded cybersecurity posture. Heightened vigilance is critical.

Executive Summary

While the physical threat of Iranian-made unmanned aerial vehicles (UAVs), or drones, has been clearly manifest in the skies over Israel, the Red Sea, and Ukraine, the industry behind these systems also poses significant challenges to global businesses and to Western governments. Insikt Group identified five major risks posed by Iran's growing drone industry related to compliance, reputation, technology transfer, global proliferation, and cybersecurity. Iran's production of drones relies on an evolving global network supporting its procurement of foreign-made components, which exposes Western defense and manufacturing companies to compliance violations and reputational harm by making it more likely that Iran could acquire their technology. Iran's established relationships with state actors and non-state proxies widen Iranian drone exports — thrusting its drone industry into a position of greater geopolitical relevance. Furthermore, Iran's ability to domestically reproduce foreign technology, driven by self-sufficiency goals, erodes the effectiveness of Western governments' regulatory regimes and heightens the cyber-espionage threat to government contractors.

Insikt Group proposes a number of measures for businesses to mitigate supply-side risk and for governments to impede Iran's illicit practices more effectively. Businesses should establish robust compliance programs and proactively seek to understand the types of equipment that Iran's drone industry needs most to advance its program, such as turbojet engines and electro-optical/infrared navigational systems, as well as the "red flag" illicit practices Iran's industry uses. Governments should continue to invest in investigative resources to identify Iran-based firms and coordinate export control efforts across an alliance of global partners. Businesses and governments should ensure robust cybersecurity practices surrounding contractors involved in the drone industry due to Iran's use of cyber espionage to enable its drone advances. Iran's drone industry enhances its economic and strategic status, and Tehran is almost certainly dedicated to sustaining the resilience of its program by adapting, despite global efforts to combat it. By leveraging partnerships with Russia and networks in Asia to produce and proliferate more advanced systems, Tehran is pushing Western industry and governments to require greater vigilance.

Key Findings

- Iran's growing drone industry utilizes complex and evolving global procurement networks and well-honed sanctions evasion techniques to acquire Western-made components, which almost certainly increases compliance-violation and reputational risk for companies manufacturing drone-related technologies or dual-use components.
- Iran has fostered an effective domestic engineering industry with a focus on producing copies of foreign-made technology, which has almost certainly eroded the effectiveness of global sanctions and export controls in halting Iran's drone development.
- The global expansion of Iranian drone exports and production — exemplified by Tehran and Moscow's cooperation — represents a growing threat, as the combined industrial expertise,

resources, and sanctions evasion experience almost certainly enhance both countries' drone capabilities.

- Iranian threat actors associated with the Islamic Revolutionary Guard Corps (IRGC) are likely seeking to leverage cyber-espionage capabilities to advance the design and production of advanced weapons, including drones, and pose a threat to defense contractors and drone-related software or component manufacturers.
- Companies should avoid compliance-violation and reputational risks by maintaining robust compliance programs, learning the "red flags" of Iranian sanctions evasion techniques, and being aware of the specific components and technology sought by Iran's drone industry.
- Governments should invest resources in identifying and targeting key entities supporting Iran's drone industry and third-country facilitators, aligning strategies, and engaging companies to improve compliance processes.
- Iran will almost certainly seek to continue reaping the strategic, military, and economic benefits of its drone industry by bolstering its domestic production and technological innovation, building bilateral relationships and enhancing its global influence through sales, and expanding its global market.

Background

Over the last year, Iranian UAVs, or drones, have proliferated as a global security threat. Iran's unprecedented April 2024 direct attack on Israel involved the launch of 170 drones, and at the start of 2024, Ukraine claimed Russia had launched over 3,700 Iranian-made Shahed drones to devastating effect on the front lines in Ukraine. Iran and its proxies have used these aircraft across the Middle East, including targeting United States (US) military bases in the region, striking critical infrastructure in Saudi Arabia and the United Arab Emirates (UAE), and attacking Western naval ships and international commercial vessels from the Red Sea to the Persian Gulf. Iran has exported drones to, or enabled production in partnership with, numerous other countries, including Ethiopia, Sudan, Venezuela, Tajikistan, Belarus, and Syria.[1] Data compiled and analyzed by the Global Terrorism Trends and Analysis Center reveals that Iran-origin drones now represent most attack drones used in the world today — even before including Russia's use of Iranian drones in Ukraine.

Iran's Strategic Prioritization of Drones

The broad use of Iranian drones across regional conflicts almost certainly reflects the strategic prioritization — at the highest levels of the Iranian government — of developing, producing, and proliferating these systems. Iran has fostered its military-industrial complex to support this national security objective. Despite sanctions imposed by the US, the United Kingdom (UK), Canada, and the European Union (EU) on entities involved in Iranian drone development, production, and proliferation, Iran has continued to manufacture, deploy, and export a wide arsenal of drones.

The Iranian drone industry responsible for this global advance comprises a multi-faceted ecosystem including government, military, and private organizations. Two key military entities drive the strategic demand for drones: the Ministry of Defense and Armed Forces Logistics (MODAFL) and the IRGC. Those military organizations oversee drone development and production through a handful of large state-owned aviation corporations. These state-run drone programs are supported by a vast and dynamic array of private companies, including engineering and production contractors, technical research and development entities, and foreign procurement firms.

[1] *https://en.irna[.]ir/news/84756555/Iran-begins-building-drones-in-Tajikistan*

Iranian Entity	Role in Drone Industry
MODAFL	• Established in 1989 to create a centralized structure for Iran's defense industries, headed by Iran's Minister of Defense • Oversees a number of state-owned defense corporations involved in aircraft and drone manufacturing through its Aviation Industry Organization • Drives drone demand through its role in the development and production of strategic military systems, including drones and foreign engagement with partners such as Russia
IRGC	• Established after the Iranian Revolution to protect and export the revolution's core principles as Iran's most powerful military and security force • IRGC's Aerospace Force, under Brigadier General Amir Ali Hajizadeh, has played a critical role in developing drone technology through an R&D program within its subordinate Shahed Aviation Industries Research Center • Drives drone demand through the export of drones to regional proxies • IRGC Quds Force (IRGC-QF), the clandestine branch of Iran's IRGC responsible for extraterritorial operations, maintains a division, known as Department 8000, which is tasked with developing and providing drones and drone-training to proxies, including the Houthis in Yemen and Iraqi and Syrian militias.
Iran Aircraft Manufacturing Industries (HESA)	• Produced the Ababil-1 in 1986 during the Iran-Iraq War and has since developed at least five versions • Manufactures the Ababil-5, which has "security, reconnaissance, intelligence-gathering, and electronic warfare capabilities", and was deployed to the IRGC Ground Forces as of February 2024[2]
Qods Aviation Industries (QAI)	• Developed Iran's first drone, the Mohajer-1, during the Iran-Iraq War • Unveiled the Mohajer-10, which has a range that can reach Tel Aviv, in August 2023 in a video that implicitly threatened Israel, with a warning in Hebrew and Persian to "Prepare your shelters" • Russia has deployed QAI's Mohajer-6 reconnaissance-strike drones against Ukrainian forces, and the UK Ministry of Defense assessed the drones were used to support "Russian targeting processes"

[2] *https://www.presstv[.]ir/Detail/2024/02/21/720473/IRGC-Ground-Force-takes-delivery-of-sophisticated-homegrown-kamikaze,-combat-drones*

Shahed Aviation Industries Research Center (SAIRC)	• Designs and manufactures Shahed-series drones — including the widely-utilized Shahed-136 one-way attack drone that was the "centerpiece" of Iran's unprecedented April 13, 2024, attack on Israel; in Ukraine, Russia has used both the Shahed-136 (renamed Geran-2) and its smaller precursor, the Shahed-131 (renamed Geran-1), according to the US Defense Intelligence Agency (DIA) • Based in Isfahan, Iran, the company reportedly operates a research, development, and production facility at Badr Air Base • First developed the Shahed-129, referred to as the "backbone" of Iran's drone fleet, in 2012 • Prolific in developing new drone technology: the turboprop engine-powered Shahed-149 Gaza, the high-altitude long-endurance Shahed-147 (allegedly comparable to the US RQ-4 Global Hawk), and jet-powered drones known as the Shahed-171 and Shahed-238

***Table 1**: Key entities in Iran's drone industry include military organizations and specialized aviation companies (Source: Insikt Group)*

International Efforts to Combat Iranian Drone Production and Proliferation

The international community has recognized the destabilizing role of Iranian drones in global conflicts and has sought to combat their production and proliferation. From multilateral regulatory regimes developed by over 30 member states to individual governments' specific export control and sanctions lists, the landscape of regulation and controls targeting the Iranian drone program is complex and dynamic. Insikt Group highlights the following non-exhaustive key regulatory regimes that are seeking to thwart Iranian drone production and proliferation.

Export Control Regime	Background
International	
Missile Technology Control Regime (MTCR)	• Established in 1987, the MTCR restricts exports of missiles and related technologies capable of delivering any type of weapon of mass destruction, including unmanned aerial systems (drones) capable of delivering a payload of at least 500 kg to a range of at least 300 km.
Wassenaar Arrangement	• Established in 1995, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies implements member nations' export controls on conventional military equipment (including drones) and dual-use items such as electronics and navigation technology.

United Nations Security Council (UNSC) Resolution 2231	• Endorsing the 2015 Joint Comprehensive Plan of Action (JCPOA, also known as the Iran nuclear deal), UNSCR 2231 prohibited Iran from the sale, supply, or transfer of nuclear-capable ballistic missiles and drones, as well as certain materials and technologies relevant to building those systems. • These restrictions expired in October 2023, but the US, UK, EU, Canada, Japan, South Korea, and other Proliferation Security Initiative-endorsing states maintained the restrictions.
United States	
US Sanctions	• US sanctions and export controls against Iran's nuclear and ballistic missile programs were established in 2005, and many of the large military entities and defense industrial organizations supporting Iran's aerospace and aviation development were designated between 2005 and 2010, prior to the emergence of the offensive drone threat.[3] • The US government specifically imposed sanctions on Iranian drone-related companies and individuals in October 2021.
Export Administration Regulations (EAR)	• Under the US Department of Commerce, EAR controls the export of commercial and "dual-use" items and technology through foreign specific export restrictions.
International Traffic in Arms Regulation (ITAR)	• Under the US Department of State, ITAR designates drones and drone-related technology or components as having a military application or controlled for national security purposes, and subject to export restrictions.
Europe and Canada	
United Kingdom	• The UK sanctioned Iranian entities responsible for supplying Russian drones in October 2022. The UK had previously designated several entities responsible for the Iranian drone program, including MODAFL, HESA, QAI, and IRGC Aerospace Force Commander.
European Union	• The EU announced sanctions specifically targeting Iranian entities supplying drones to Russia in October 2022.

[3] For example, the US Department of the Treasury sanctioned the IRGC Aerospace Force (IRGC ASF) in June 2010, and IRGC and MODAFL in October 2007. Those organizations were designated pursuant to Executive Order 13382, which targeted proliferators of weapons of mass destruction (WMD) and their means of delivery.

Canada	• Canada designated over 300 Iranian entities and persons "for grave breach of international peace and security" under its Special Economic Measures Act in 2010, including some companies involved in drone production or development. The Act has been amended on multiple occasions to impose sanctions on drone-related entities.
Switzerland	• Switzerland adopted EU sanctions imposed on entities involved in Iranian drone supply to Russia in 2022.

Table 2: *Non-exhaustive list of multilateral and nation-state regulatory regimes pertaining to Iranian drones (Source: Insikt Group)*

Key Risks Posed by Iran's Domestic Drone Industry

Insikt Group compiled and analyzed information about the Iranian drone industry published by the US, UK, EU, and Canadian governments' sanctions or regulatory compliance agencies; United Nations (UN) expert analysis and independent journalist investigations of Iranian drones and their components; Iranian government, military, and state-run news media announcements regarding drones; and information on Iranian drone production revealed by alleged hackers. These sources illuminate the illicit activities, networks, transactions, tactics, and techniques enabling Iran's drone industry, and Insikt Group has analyzed case studies to depict these specific risks. While the deployment and operational use of Iranian drones pose a well-documented physical security threat to personnel or infrastructure, this analysis focuses instead on five other risks to both governments and businesses posed by Iran's growing drone industry, including compliance risk, reputational risk, technology transfer risk, global proliferation risk, and cybersecurity risk.

Compliance Risk: Iran's Illicit Procurement Networks

A review of US government information on Iran's procurement activities — including export control guidelines, US Department of the Treasury sanctions designations, and violations documented through US federal and state indictments and convictions — brings into focus the type of entities, practices, transactions, and networks sustaining the Iranian military aviation industry. Iran's drone programs rely on foreign-made components, which it obtains through an illicit web of front companies, dual-use component suppliers and middlemen, logistic transport companies, and financial exchange brokers. These enabling entities are established in Iran and in non-Western countries, including in Asia and the Middle East, that lack international sanctions enforcement. Leveraging mainland Chinese suppliers and distributors, in particular, as well as suppliers and distributors in Hong Kong, Malaysia, and Indonesia, is likely a favored mechanism by which Iran sources foreign components. Companies based in the UAE have been sanctioned for shipping facilitation, and Türkiye-based companies have been implicated in facilitating financial transactions for component procurements. Commonly used "red flag" tactics and schemes include:

- Obscuring the ultimate destination and end user through a global network of procurement agents, resellers, intermediaries, or front or shell companies
- Falsifying end-user or shipping documentation to avoid export control scrutiny
- Sending and receiving payments through foreign banks or third-party businesses, including shell companies, outside the company's jurisdiction to obfuscate the source of funding
- Using atypical or conspicuously indirect shipping routes for a product and destination, or routing through common illicit transshipment points

Due to the wide range of illicit entities involved in the drone program, the landscape of potential risks for private companies unknowingly or unintentionally enabling the Iranian drone industry has almost certainly increased. Enforcement of obligatory compliance regulations can have substantial legal and monetary ramifications on individuals and businesses, as can failure to implement effective controls. While the UK, the EU, and Canada each have different compliance regimes and related enforcement mechanisms, the collective regulatory environment seeking to curb the Iranian drone industry is likely to remain a Western policy priority and increase both enforcement and transatlantic cooperation. For example, the US Congress is considering a bill, H.R. 1809, "Block the Use of Transatlantic Technology in Iranian Made Drones Act", which would require the US Department of Commerce to "develop a strategy to supplement the existing US sanctions regime against Iran by preventing the export to Iran of certain technologies (including microcontrollers, voltage regulators, and microprocessors) that can be used in the development and employment of UAS [unmanned aircraft systems]", and mandate the US Department of State to "develop a strategy to engage European and Asian allies and partners to prevent the export of these technologies". Greater enforcement of regulatory regimes will very likely be a key factor in combating the trend of widening production and proliferation of Iranian drones.

Case Study: The Ardakani Network

According to US government information, Iranian national Hossein Hatefi Ardakani led an international procurement network that obtained US-origin, dual-use, and sensitive technology used in Iranian drones for IRGC's Aerospace Force. Based on US Department of the Treasury sanctions information, the IRGC Aerospace Force Self Sufficiency Jihad Organization (IRGC ASF SSJO) directly contracted with Ardakani, who used firms and front companies in Iran, Hong Kong, Malaysia, and Indonesia to acquire various drone-related components, including servomotors, fuel pumps, antennas, spectrum analyzers, gas thrusters, and modular measurement systems. This network (**Figure 1**) is very likely representative of the type of complex, multi-faceted mechanism relied upon by the Iranian drone program.

Ardakani's criminal indictment revealed his Chinese partner, Gary Lam, and their associates used unwitting French and Canadian companies to purchase, acquire, and then ship US-made microelectronics to Hong Kong and China. From Asia, the components were then re-exported to Iran. The illicit shipments included export-controlled goods, such as high electron mobility transistors, monolithic microwave integrated circuit power amplifiers, and analog-to-digital converters — all of which are commonly used in UAV production. Ardakani and Lam used a combination of witting and unwitting French, Canadian, Hong Kong, and Chinese companies to mask the ultimate destination of goods.

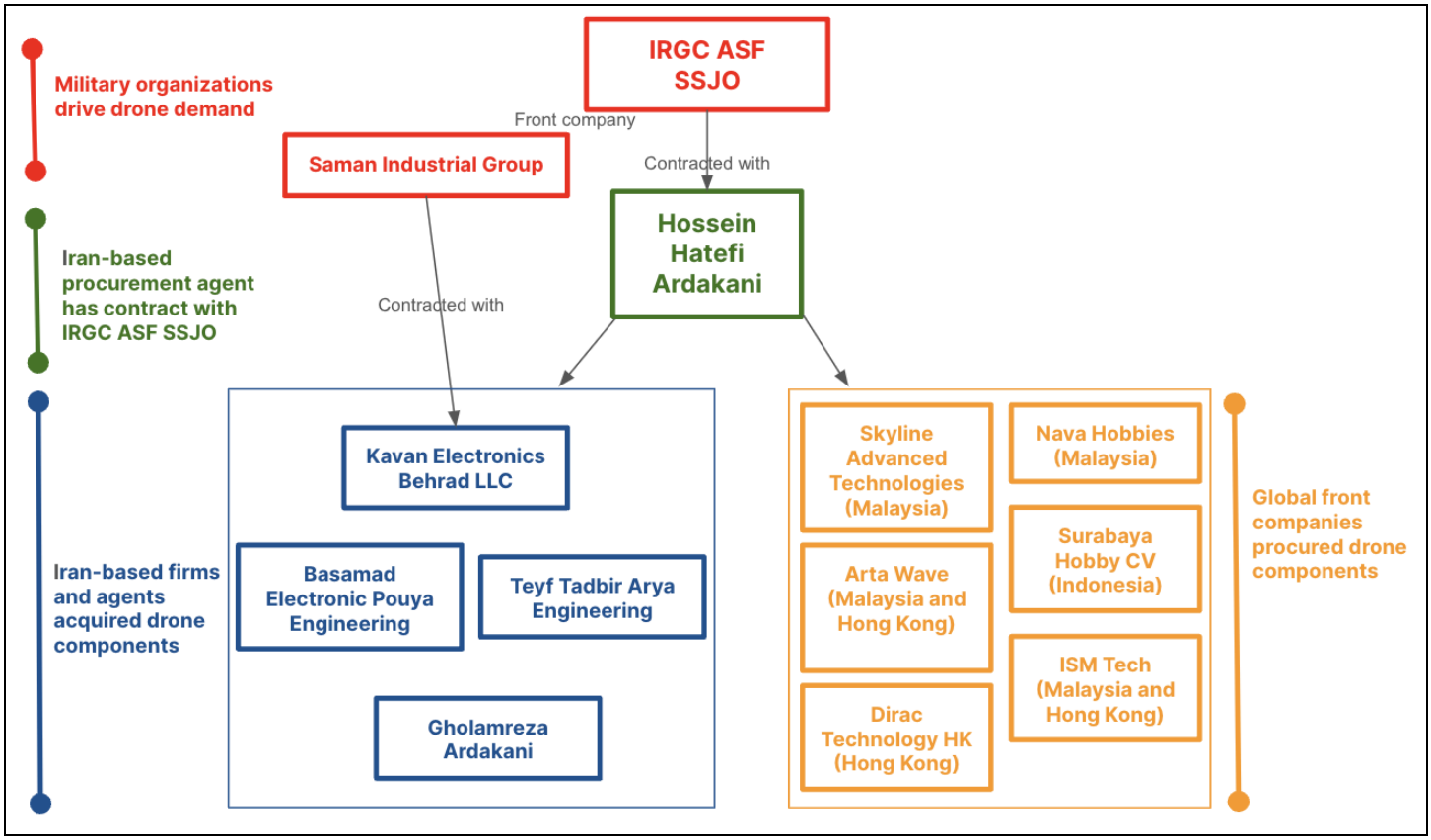


Figure 1: *Network diagram of Ardakani's global procurement network, based on US Department of the Treasury Office of Foreign Assets Control (OFAC) designation information (Source: Insikt Group)*

Case Study: Edsun Equipment's Export Falsification and Smuggling

From May 2015 to October 2017, a New Jersey-based aviation parts trading company, Edsun Equipment LLC, facilitated the smuggling of over 20,000 controlled aircraft parts in nearly 50 shipments — worth over $2 million — to Iran. According to New Jersey District Court documents, the company's principal operator knowingly falsified the true destination and value of the aircraft components to obscure the end users and avoid filing export control forms. The convicted facilitator, a naturalized US citizen born in the Philippines, ordered specifically requested components from US-based distributors, repackaged them, and shipped them using US-based shipping companies to freight forwarders in UAE and Türkiye, for onward delivery to Iran. The US citizen conspired with an Iranian national, Peyman Amiri Larijani, whose Iranian clients included US-designated Iranian airline Mahan Air. The Iranian clients paid for the components by funneling funds through Turkish bank accounts held by Iranian shell companies, concealing the true origin of the funds. Although Mahan Air and other entities that benefited from Edsun's scheme were not specifically building Iranian drones, the smuggling and payment mechanism used in this case almost certainly could be used to acquire drone parts.

Reputational Risk: Western Components in Deadly Drones

Even as countries with major defense manufacturing industries have developed export control and sanction regimes, illicit procurement mechanisms have enabled Iran to acquire American, Canadian, European, and Japanese parts from global distributors. Iran's ability to acquire these parts — and use them in Iranian drones — poses a reputational risk for technology companies whose products are found in Iranian drone wreckage in conflict zones.

Western-made parts identified in Iranian-made drones are often mass-produced (rather than custom-made), relatively inexpensive, and widely accessible through commercial off-the-shelf vendors. Iran almost certainly leverages overseas distributors or resellers — sometimes through multiple transactions — to put distance between the initial export license-approved commercial sale and the ultimate Iranian end user. Some key drone components are dual-use and small, such as circuit board components, GPS or navigational equipment, microchips, microprocessors, and microcontrollers — which are more easily smuggled, or acquired and resold through various levels of distributors. Multiple layers of transfers make it difficult to track the items after initial export. Many are "low-technology items" that are not included in the US Commerce Department's export control list.

In addition to the penalties associated with compliance failure for technologies that are controlled, the use of Western parts in Iranian drones almost certainly leaves both companies and governments vulnerable to criticism and reputational harm. For companies, this trend could be framed as a result of companies' negative intent or compliance inadequacy. According to Moody's Analytics research published in April 2023, 69% of businesses said they lacked the necessary visibility over their supply chains to uncover risk in their organization and avoid reputational harm. For Western governments, the Iranian drone industry's ability to incorporate a broad array of Western-made parts raises questions about the overall effectiveness of their export control policies and casts doubt on the regulatory enforcement mechanisms underpinning those policies. Even with increased pressure on Iran's drone program — through additional sanctions, greater enforcement of export controls, and greater awareness by companies — Iran will likely maintain mechanisms to obtain Western-made parts, and the risk that both governments and companies will face criticism or reputational damage will therefore persist.

Case Study: Western Components Identified in Iranian Drones Used In Ukraine

In late 2022, Ukrainian intelligence reported to the US government on the prevalence of US-made parts in Iranian drones used by Russia. According to the Ukrainian assessment, 40 of the 52 components in a downed Shahed-136 drone were manufactured by 13 different US companies; components made by Swiss, Japanese, Taiwanese, and Chinese companies were also identified. A similar study conducted in 2022 by the UK-based investigative organization Conflict Armament Research (CAR) examined over 500 components across five Iranian-made drones. That analysis revealed that over 85 manufacturers from 13 countries produced Iranian drone components — with 82% manufactured by US-based companies. While CAR has not published the full list of over 70 manufacturers identified in its analysis,

an August 2023 report by the Yermak-McFaul International Working Group on Russian Sanctions published a list of 36 manufacturers of 109 components found in Shahed-131 and Shahed-136 drones retrieved in Ukraine, of which over two-thirds were US-based companies (**Figure 2**). According to an analysis by the Institute for Science and International Security, predominantly Western-made components "lie at the heart of the Shahed-136's ability to evade Ukrainian jamming and reach their targets".

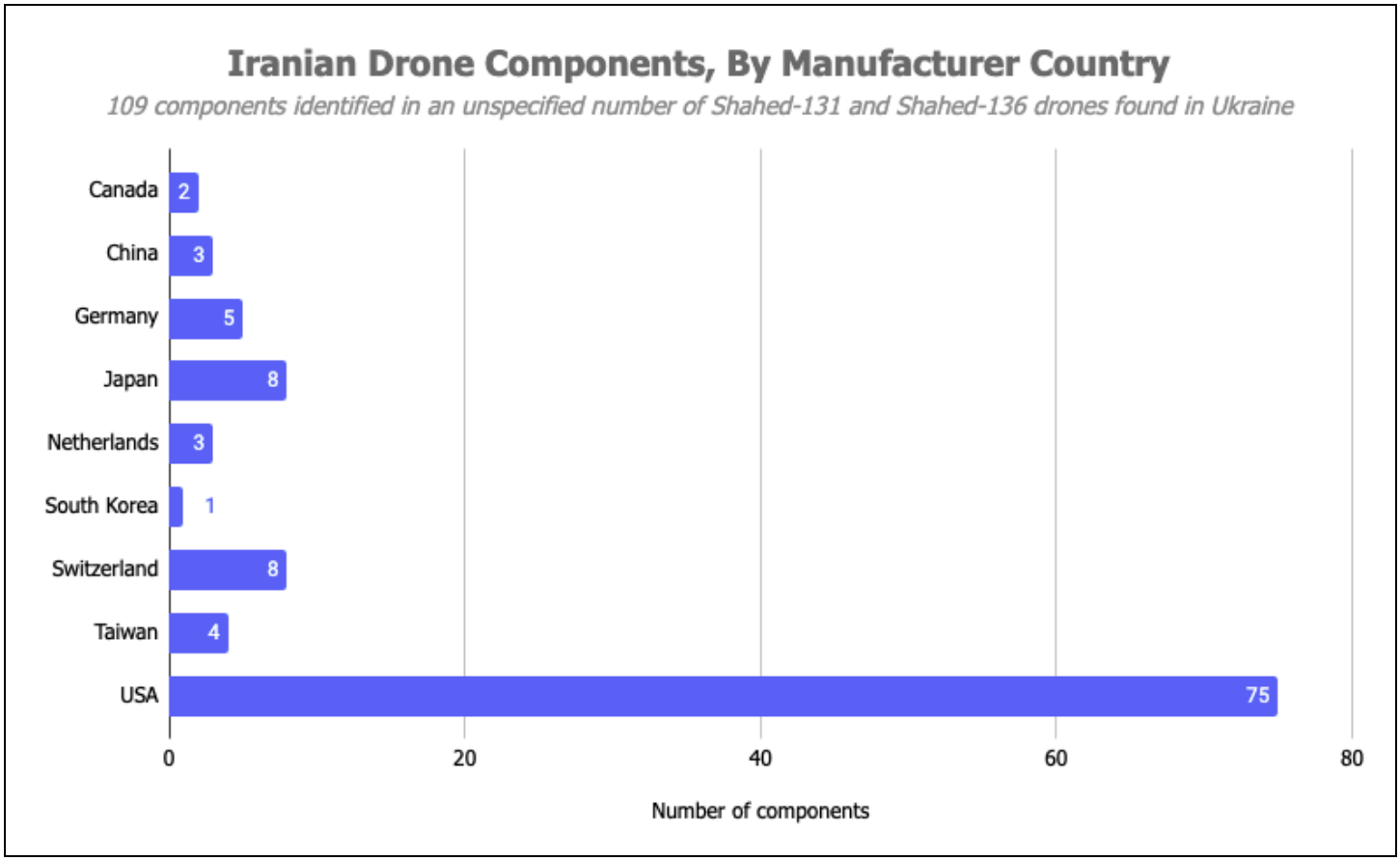


Figure 2: *Chart showing the manufacturer's country for 109 components identified in an unspecified number of Shahed-131 and Shahed-136 drones in Ukraine (Source: Yermak-McFaul International Working Group on Russian Sanctions)*

In the wake of the revelation of US-made parts in Iranian drones, the identified private companies — including Texas Instruments, Hemisphere GNSS, NXP USA, Analog Devices, and Onsemi — vehemently defended their adherence to export control laws and regulations. Several companies reinforced their efforts to prevent illicit activity, such as Massachusetts-based Analog Devices, which said it was "implementing enhanced monitoring and audit processes, and taking enforcement action where appropriate". According to experts, controlling the transfers of these "highly ubiquitous parts" is often very difficult, and these companies have not faced legal repercussions or financial penalties, at least publicly.

However, the revelations about their products in Iranian drones exposed these companies to reputational damage resulting from public criticism. In social media and messaging forums, critics

blamed these companies for being complicit in inadvertently helping Iran or failing to adhere to sanctions or export controls. As an example of the type of criticism companies faced in the wake of the revelations, a social media user posted in November 2022, "It's disgusting that Western companies are going around Sanctions to provide Iran (brutal regime) with parts to make drones to give to Russia (another brutal regime) to attack Ukraine. The WEST must wise up and #DoTheRightThing #Shameful". Another user alleged that Texas Instruments illegally sold components to Iran and was "war profiteering off of dead Ukrainians in favor of Putin", including the hashtag #sanctionTexasInstruments in their post. Another user criticized US Speaker of the House Nancy Pelosi, tagging @SpeakerPelosi, for pushing "massive TAX BREAKS for companies like TEXAS INSTRUMENTS" while "TI w/ other manufacturers are SUPPLYING NECESSARY COMPONENTS TO MAKE IRANIAN KAMAKAZI [sic] DRONES Where are SANCTIONS for aid to Iran?" In response to a US Department of the Treasury sanctions announcement in January 2023 targeting Iranian drones used in Ukraine, a user posted, "What I didn't see was any mentions of actions against any US companies selling those parts to Iran", suggesting the US should be "taking the appropriate actions and shutting down that pipeline of parts".

Companies have faced scrutiny from both government authorities and independent watchdogs for failing to prevent their parts from being exported to Iran. Tonegawa Seiko, a Japanese company that produces servo motors, was investigated by Japanese authorities for exporting 150 servo motors to China with no permit in June 2020, under suspicion of violating Japan's Foreign Exchange and Foreign Trade Law. The motors were found in an Iranian-made drone that crashed in Afghanistan in 2016 and in shipments bound for Yemen in 2018 and 2020 that were seized by UAE authorities, according to a UN report. In December 2022, US president Joe Biden launched a task force to investigate the prevalence of US-made components in Iranian drones found in Ukraine. US Congress members reportedly sought the list of US companies whose equipment is being found in drones "to force greater accountability by urging the companies to monitor their supply chains more closely". Sixty Congress members wrote a letter, addressed to the US president and secretaries of state, commerce, and the treasury, requesting a "coordinated, whole of government approach" to address the issue, including "to crack down on unscrupulous distributors in Europe and Asia". The president of the Canada-based firm Tallysman Wireless stated that his company was cooperating with Canadian government agencies after learning its antennas were in Iranian drones, defending his company by noting, "It is sometimes assumed that we are somehow complicit in this usage". Bombardier Recreational Products, another Canadian company that produces engines used in Iranian drones, conducted an internal probe and shared the report with the Canadian authorities for their further investigation.

Companies are also placed in a position of defending both their compliance practices and their political values as non-governmental entities publicize the companies that make Iranian drone parts. Experts from Ukraine's Anti-Corruption Commission (NAKO) — an independent organization working to reduce corruption in the Ukrainian national security sector — sent over 35 letters to companies with parts in Iranian drones. The Business & Human Rights Resource Centre, based in London, England, published German semiconductor manufacturer Infineon's response to the revelation, which asserted the company's position condemning "the Russian aggression against Ukraine", reinforced its willingness to "continue to do our part as a company to support the victims of this conflict [with Russia]", reassured that "compliance with applicable laws is of utmost importance for Infineon", and noted, "it proves

difficult to control consecutive sales throughout the entire lifetime of a product". Non-profit United Against a Nuclear Iran (UANI) contacted Taiwanese company ATEN International raising concerns over the company's business with a Tehran-based firm linked to the IRGC, prompting ATEN to immediately stop accepting orders from the Iranian company. Company investors are also ramping up engagement with electronics firms; shareholders of Arizona-based Microchip Technologies voted in favor of its board of directors commissioning an independent third-party report on its due diligence process "to determine whether its customers' use of its products contribute to or are linked to violations of international law".

Figure 3: *Screenshot of video of Ukrainian president Volodymyr Zelensky with a downed Iran-produced Shahed drone after a Russian barrage of over 30 drone attacks in two days, in October 2022 (Source: BBC)*

Likewise, the US, Canadian, and European governments faced criticism for perceived ineffectiveness in their ability to identify and prevent such illicit activity involving US or European companies. For example, in November 2022, a social media user posted criticizing the prevalence of US-made parts, saying, "what a failure on US part that has missed these". Users directly urged US government actions through social media, such as a user that tagged @POTUS, @SecBlinken, and @StateDept saying, "Please check how Iran manages to use Intel chips to build suicide drones, and make sure it stops". One user inquired of US Secretaries of Defense and State, "Will there be any aggressive steps against embargoed Iran providing sanctioned russia with missiles and suicide drones?", while another user, former US Department of State advisor for the Iran Action Group Gabriel Noronha, said, "We [the US] have got to get better about export controls, end-use monitoring/reporting, and sanctions". In November 2022, another user posted a message directed at Secretary of State Antony Blinken

(@SecBlinken), saying, "You are a liar. #America and #Canada secretly gave parts of suicide drones to Iran to produce drones and send them to #Russia to kill the oppressed people of Ukraine. All your sanctions are like jokes".

Technology Transfer Risk: Reverse Engineering and Mass Production

Iran's ability to innovate in drone production, despite years of global sanctions and economic isolation, is a testament to the Islamic Republic's dedication to its domestic manufacturing industry and the abilities of the research and development companies that support it. In parallel with Iran's global procurement networks bringing in foreign parts, Iran has fostered a robust defense industry to drive the research and development, engineering, and technical requirements for drones. A review of companies identified in US and European sanctions, UN investigations, and independent expert analyses suggests these companies produce drone airframes and specialized components often by reverse-engineering Western-origin versions. The companies that wittingly support this effort pose a threat to international security as they are instrumental in closing the gap between Iran's componentry demands and its production capabilities — and almost certainly erode the effectiveness of global sanctions and export controls in halting Iran's drone development.

Iran's drone program exemplifies one of the Islamic Republic's core national security objectives — self-sufficiency. In March 2024, Iranian defense minister Mohammad Reza Ashtiani asserted Iran had "achieved self-sufficiency in the field of making drone engines" while endeavoring to "reach higher levels in manufacturing heavier engines".[4] Iran's alleged progress in its drone engine manufacturing very likely reflects a larger trend — that Iran is building its domestic industry by cloning. Two case studies detailed below underscore the threat of Iranian industries' reverse engineering of technology produced by foreign countries in industrialized nations, such as the US, UK, EU, Israel, and Japan. Iran is almost certainly seeking to grow its indigenous engineering capabilities through companies like Mado, discussed below, amplifying the risk that Iran is increasingly self-sufficient and less reliant on Western export-controlled goods.

Case Study: Mado Company's Copy of European Engines

Oje Parvaz Mado Nafar Company (referred to as Mado), an Iranian-owned-and-operated company established in 2013, has played a key role in the procurement and production of Iranian drone engines. The US sanctioned Mado in October 2021 based on the company's procurement of engines for both QAI and HESA. Analysis of the wreckage of Iranian-made drones used by Russia in Ukraine, first published in April 2023, further revealed Mado's role as a manufacturer of engines used in Shahed drones. According to an investigation by CAR, Mado has reverse-engineered European-made engines, including the German-made Limbach L-550 and the UK-made AR-741 Wankel engine.

Mado engines were reportedly copied after the illicit export of German engines to Iran in 2006. Starting in 2007, Iranian engineer Yousef Aboutalebi reportedly supervised a project to develop a 25-horsepower engine using American, British, or German technology. By 2008, Aboutalebi's unnamed

[4] *https://www.presstv[.]ir/Detail/2024/03/13/721815/Iranian-defense-minister-military-equipment-significant%C2%A0rise*

company (later to be called Mado) claimed it had domestically produced the same type of drone engine. According to The Wisconsin Project on Nuclear Arms Control's IranWatch, Aboutalebi reportedly established a Hong Kong-based firm, Mado Import and Export Company Limited, in October 2013. The company dissolved in July 2019, based on Hong Kong business records, and there is limited information about Aboutalebi's role with or use of these companies.[5] However, it is possible that Aboutalebi used this Hong Kong trading company to acquire goods or materials needed for engine production. Mado's business model — illicitly acquiring Western parts in order to copy them — likely reflects a mechanism commonly used within Iran's drone industry to develop export-controlled components. It also highlights the risk that companies manufacturing or selling such components can inadvertently provide technology to Iran, which Iran's defense industry will then seek to copy.

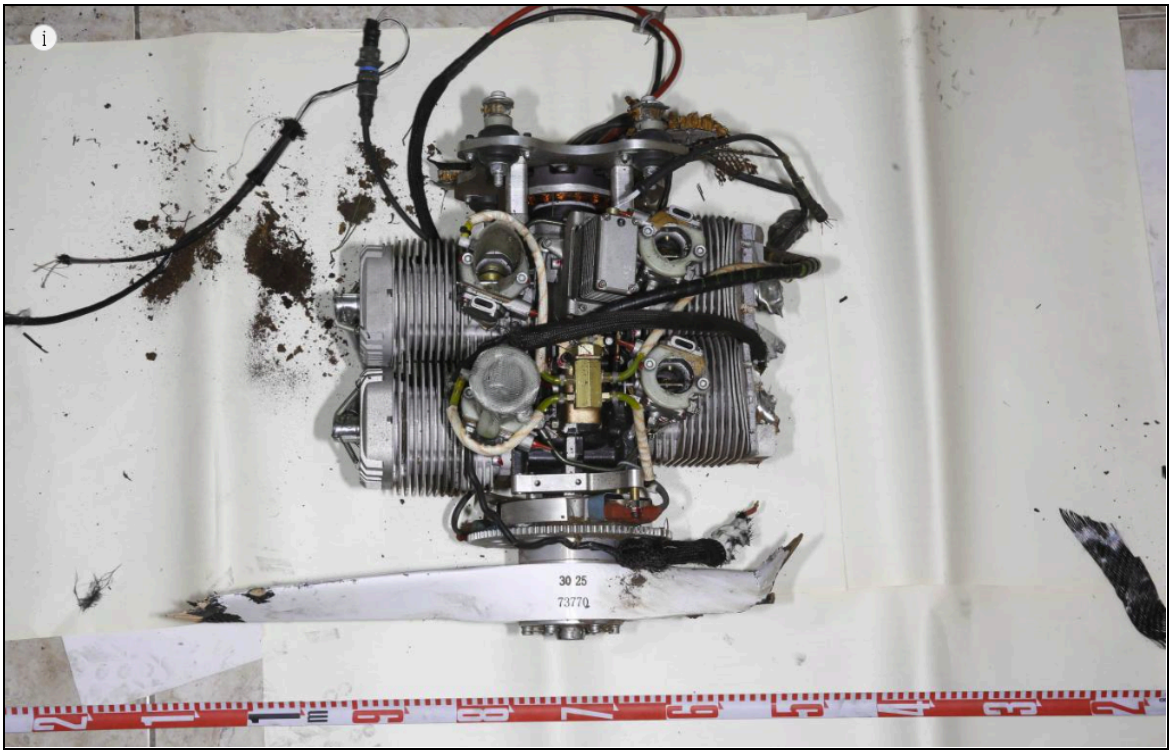


Figure 4: *A Mado MD-550 engine recovered in Ukraine used in a Shahed-136 drone — a reverse-engineered copy of a German-made Limbach L-550 engine (Source: Conflict Armament Research)*

Case Study: Iranian Copy of Downed RQ-170

In December 2011, Iran captured a US RQ-170 Sentinel drone flying over Afghanistan. Iranian officials claimed its electronic warfare unit gained control of the aircraft and brought it down, with minimal damage, in northeastern Iran; US officials indicated the aircraft went down due to a technical malfunction. The IRGC Aerospace Force commander, Brigadier General Amir Ali Hajizadeh, asserted Iran had "completely decoded and extracted" all the intelligence from the drone. By November 2014, IRGC reportedly conducted a test flight of its own version; it also claimed to have developed an attack

[5] *https://www.ltddir[.]com/companies/mado-import-and-export-company-limited/*

version in October 2016. In 2018, Israel shot down an Iranian drone — a Shahed-171 — that a senior Israeli Air Force officer described as essentially a duplication of the RQ-170.

Figure 5: *IRGC Aerospace Force commander, Brigadier General Amir Ali Hajizadeh, showing Supreme Leader Ali Khamenei the allegedly captured US RQ-170 drone and its Iranian copy, the Shahed-171, at a ceremony in May 2014 (Source: Leader[.]ir[6])*

This incident inaugurated a larger campaign by Iran's military industry to acquire and reverse engineer foreign drone designs to bolster its own industry. Analysts have identified at least three cloned versions of the RQ-170 Sentinel. The IRGC Aerospace Force has also attempted to copy various other US and Israeli airframes, including the RQ-4 Global Hawk, MQ-1 Predator, and Hermes 450. According to a regional expert, Hajizadeh received the blessing of Iran's Supreme Leader Ali Khamenei to build Iran's drone program in 2011, and Iran has acquired up to eight foreign drones shot down in Iraq, Syria, and Iran in support of that objective.

Proliferation Risk: Global Export and Production

In March 2024, Iranian defense minister Mohammad Reza Ashtiani claimed that Iranian defense exports have increased by "four to five times" since 2022.[7] Iran reportedly sold about $1 billion in weapons from

[6] *https://www.leader[.]ir/fa/media/11770*
[7] *https://www.presstv[.]ir/Detail/2024/03/13/721815/Iranian-defense-minister-military-equipment-significant%C2%A0rise*

March 2022 to March 2023 — tripling its sales from the previous year — and drones were almost certainly a significant factor in that profit. Iranian drone exports now have a global reach, beyond Tehran's regional proxies — Hezbollah in Lebanon, Iraqi and Syrian Shi'ite militias, and Yemen's Houthis — to European, African, South American, and potentially Asian theaters. The proliferation of Iranian drone technology almost certainly amplifies the risk that destabilizing drone warfare tactics similar to those used by Iran and its proxies against Israeli and US targets become more prominent in global conflicts. Characterized by "a potent mix of efficacy and affordability", Iranian drones capitalize on the relatively low cost of the systems to employ asymmetric attack tactics, such as swarming to overwhelm an adversary's air defenses and one-way "kamikaze" attacks.

Russia's purchase of Iranian drones since 2022 is almost certainly a major factor in this export surge, and Russia has used Iranian Shahed-series drones to great effect as a military tactic against Ukraine, particularly to destroy critical infrastructure. In the Middle East, Iranian drone technology has been used in fatal attacks, including the January 2024 attack on Tower 22 in Jordan, which killed three US service members, and on the Mercer Street oil tanker in 2021, which killed the vessel's Romanian captain and a British bodyguard. Iran has also exported its drone technology outside of the Middle East theater, to buyers in Armenia, Ethiopia, Sudan, and Venezuela. Iranian Mohajer-6 drones have reportedly provided a decisive advantage to the Sudanese Armed Forces over their paramilitary adversary, the Rapid Support Forces (RSF). North Korea may possess, or be interested in acquiring, Iranian drone technology to threaten South Korea and Japan. Belarus and Bolivia have also expressed interest in obtaining Iranian drone technology.

Beyond foreign sales, Iran has developed foreign production capabilities to support the growing international demand. To address Russia's requirements, Iran and Russia have jointly built a production line in Tatarstan, Russia — anticipated to produce 330 to 350 Russian-made versions of Shahed-131 and -136 drones, referred to as Geran-1 and Geran-2, each month, according to Ukrainian military intelligence. Iran has also reportedly established a factory in Syria that ships drones to the Russian port of Novorossiysk. Unconfirmed expert analysis suggested Iran was producing drones in Venezuela in 2022, to augment its supply to Russia. Iran reportedly discussed establishing a production facility in Belarus, which would further support Russia's ability to deploy Iranian drones in Ukraine.

Even prior to the heightened demand from Russia, Iran had begun to expand the production of its drones beyond its borders. Tehran reportedly opened its first extraterritorial production line in 2022 — an Ababil-2 drone factory in Dushanbe, Tajikistan.[8] According to an expert at the Washington Institute for Near East Policy, Iran's proxies maintain undeclared drone production facilities that function more like "limited production workshops", noting Lebanese Hezbollah and Yemeni Houthis "might have the largest (underground) Iranian drone production facilities outside of Iran itself". This diversification of production lines likely allows Iran to benefit economically from the global demand for its drones, while not depleting its domestic production capacity that supports its own military and national security objectives. Overseas facilities also enable sanctions evasion by decentralizing production, shortening supply chains, and easing the logistical burdens of shipping complete drone airframes. They also

[8] *https://www.tasnimnews[.]com/en/news/2022/05/17/2712404/iran-opens-military-drone-factory-in-tajikistan*

mitigate the risk of Israeli or US disruption efforts, such as cyberattacks or kinetic strikes capable of targeting Iran's domestic facilities or infrastructure. As such, the broadening of Iranian production capacity very likely dilutes the effectiveness of Western sanctions and increases the risk that Iran's componentry procurement and production processes are uninhibited.

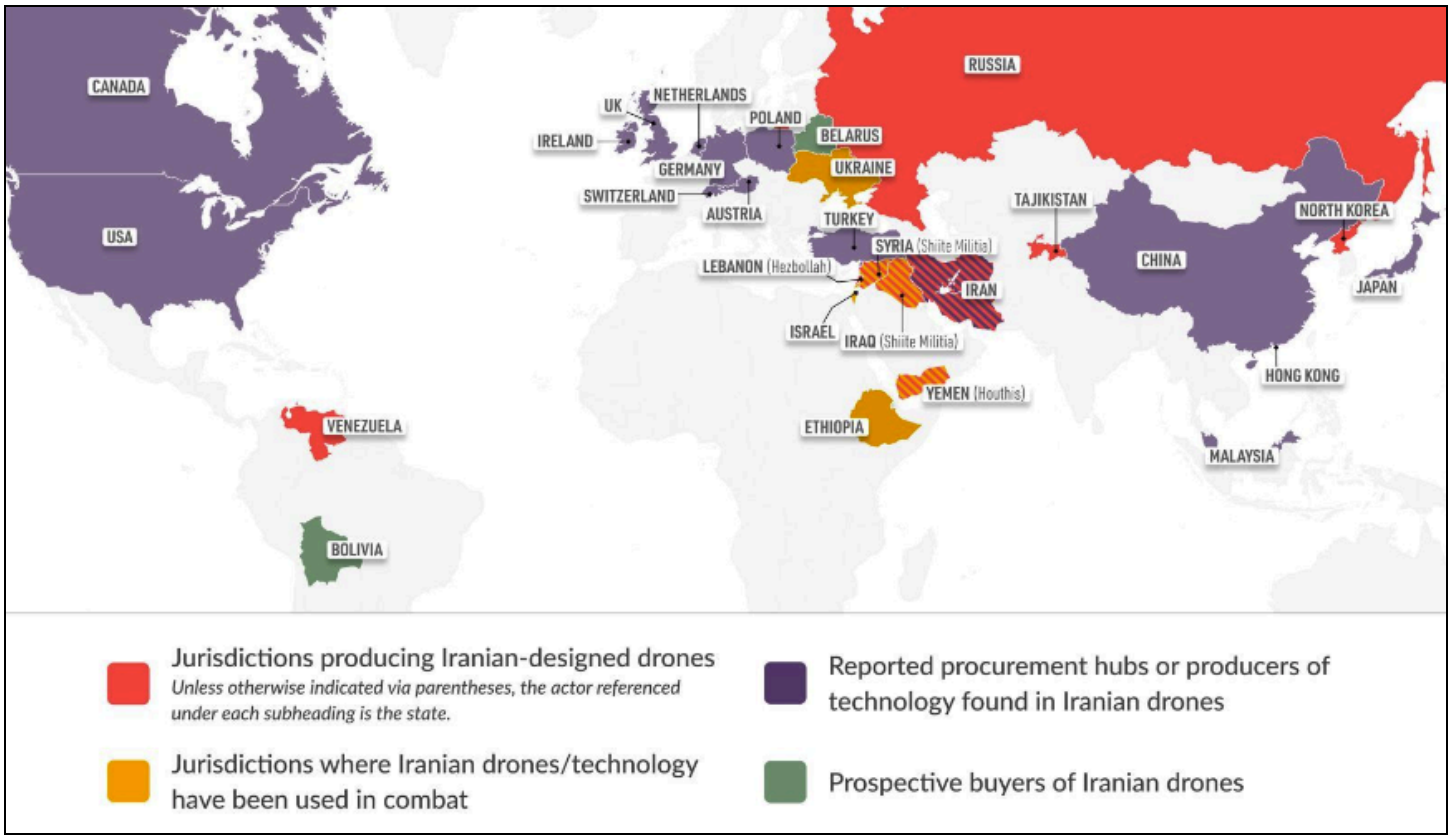


Figure 6: *Map depicting the proliferation of Iran's drone technology, including procurement and production hubs (Source: Foundation for Defense of Democracies)*

Case Study: Iran-Russia Joint Production Advances Drone Capabilities

Reporting by the Washington Post in November 2022 first revealed that Iran and Russia had jointly developed a manufacturing facility inside Russia, with the goal of producing 6,000 drones by the summer of 2025. Tehran and Moscow have established a factory at the Alabuga Special Economic Zone in Russia's Tatarstan region, almost certainly seeking to substantially enhance Iran's manufacturing capabilities — by increasing the scale of industrial production and also improving the drone technology itself — and potentially enabling "a drone developmental capability that exceeds Iran's". Analysis by the Institute for Science and International Security, published by the Washington Post, revealed a three-stage plan **(Figure 7)** involving reassembly of Iranian-made drones evolving into production of airframes, and finally advancing to independent sourcing and production in Russia.

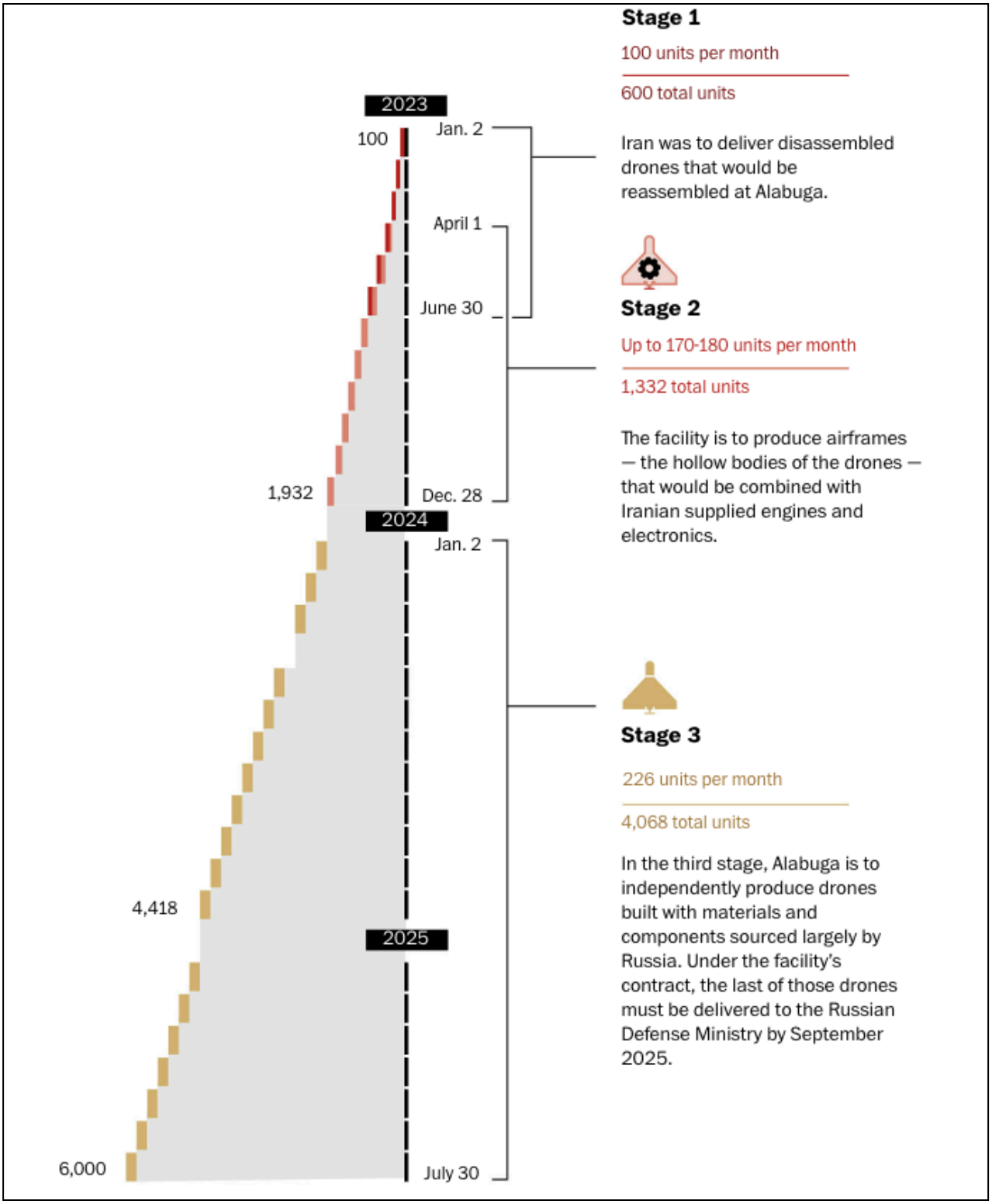


Figure 7: *Iran and Russia's three-stage joint production plan for manufacturing drones at the Alabuga facility in Russia (Source: Washington Post)*

Iran's cooperation with Russia to produce drones reflects the serious threat posed by the global expansion of Iranian drone production: the combined industrial expertise, resources, and sanctions evasion experience shared between Russia and Iran almost certainly enhances the two countries' drone capabilities. In addition to the sheer volume of drones the Alabuga facility is slated to produce — as demonstrated by the ambitious production goals — the industrial partnership and cooperation are likely enabling technological advancement in the drones' systems.

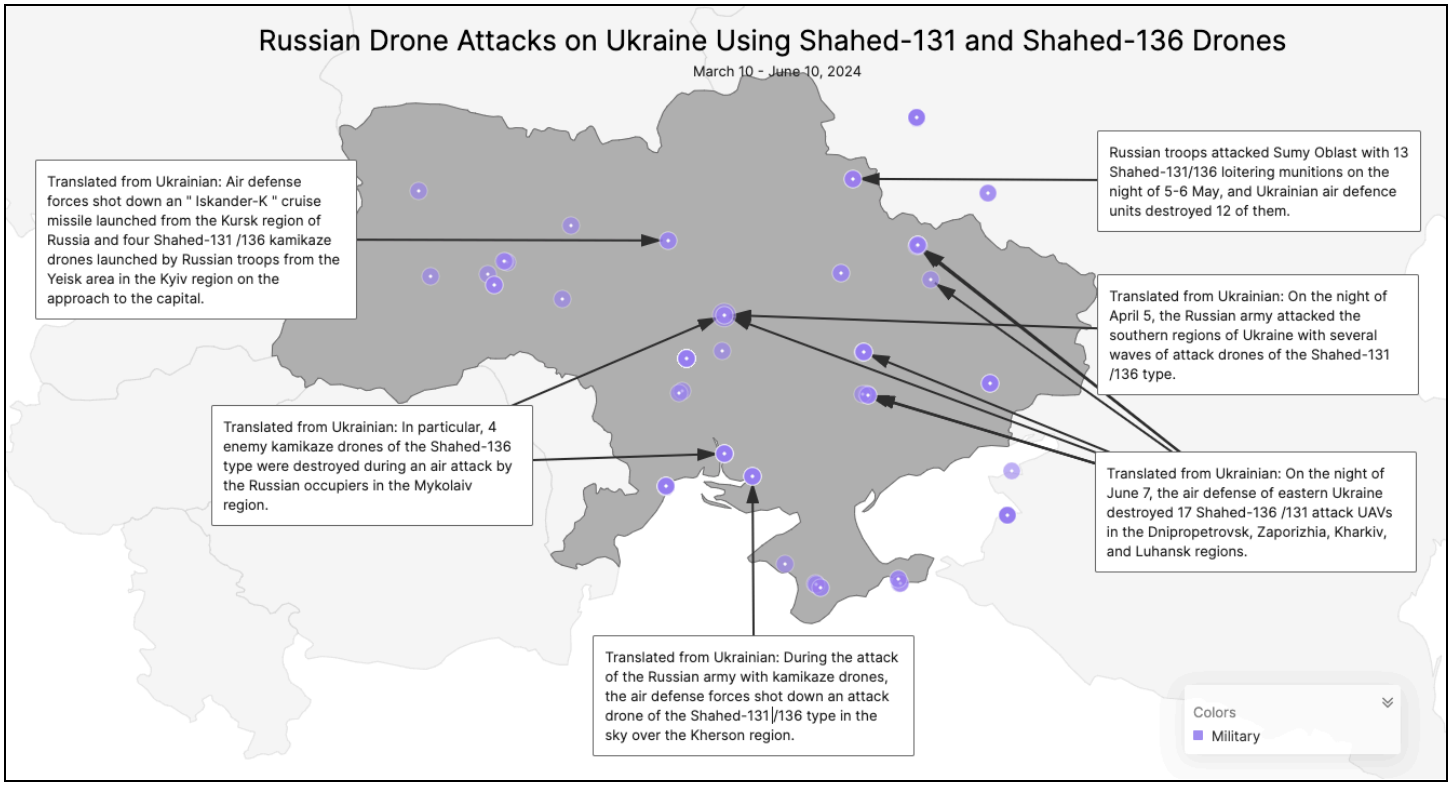


Figure 8: *Recorded Future Intelligence Cloud Query showing the non-exhaustive list of locations of Russian attacks on Ukraine using Iranian Shahed-131 and Shahed-136 drones between March 10 and June 10, 2024 (Source: Recorded Future)*

On February 4, 2024, a cyber threat actor group known as Prana Network announced it gained access to email servers allegedly used by an IRGC-affiliated weapons facilitation company, Sahara Thunder, and published alleged internal documents about Russia-Iran drone cooperation.[9] [10] Among the thousands of documents leaked were details of the production processes, contracts, and summaries of Russian officials' visits to Iran. Notably, these documents revealed details about Iran's cooperation with Russia in producing more advanced versions of its current arsenal, including the jet-powered Shahed-238 (which Russians refer to as M237) (**Figure 9, below**). An upgrade to the ubiquitous Shahed-136, the Shahed-238 can allegedly fly at 600 kilometers (370 miles) per hour, a vast improvement over the 170 kilometers-per-hour speed of the Shahed-136's piston engine. The documents revealed Russia's interest in buying 700 of the new Shahed-238 drones at an estimated cost

[9] *https://irancybernews[.]org/irgc-front-company-sahara-thunder-hacked-by-prana-network/*
[10] Prana Network identified Sahara Thunder as an IRGC-affiliated front company. In April 2024, the US Department of the Treasury OFAC designated Sahara Thunder as a subordinate to MODAFL.

of $1.4 million, as well as 2,000 of the $900,000 optically guided MC-236 drones. In February 2024, the Ukrainian military shot down a Shahed-238, indicating Russia's deployment of these new, faster models to the Ukraine battlefield in early 2024.

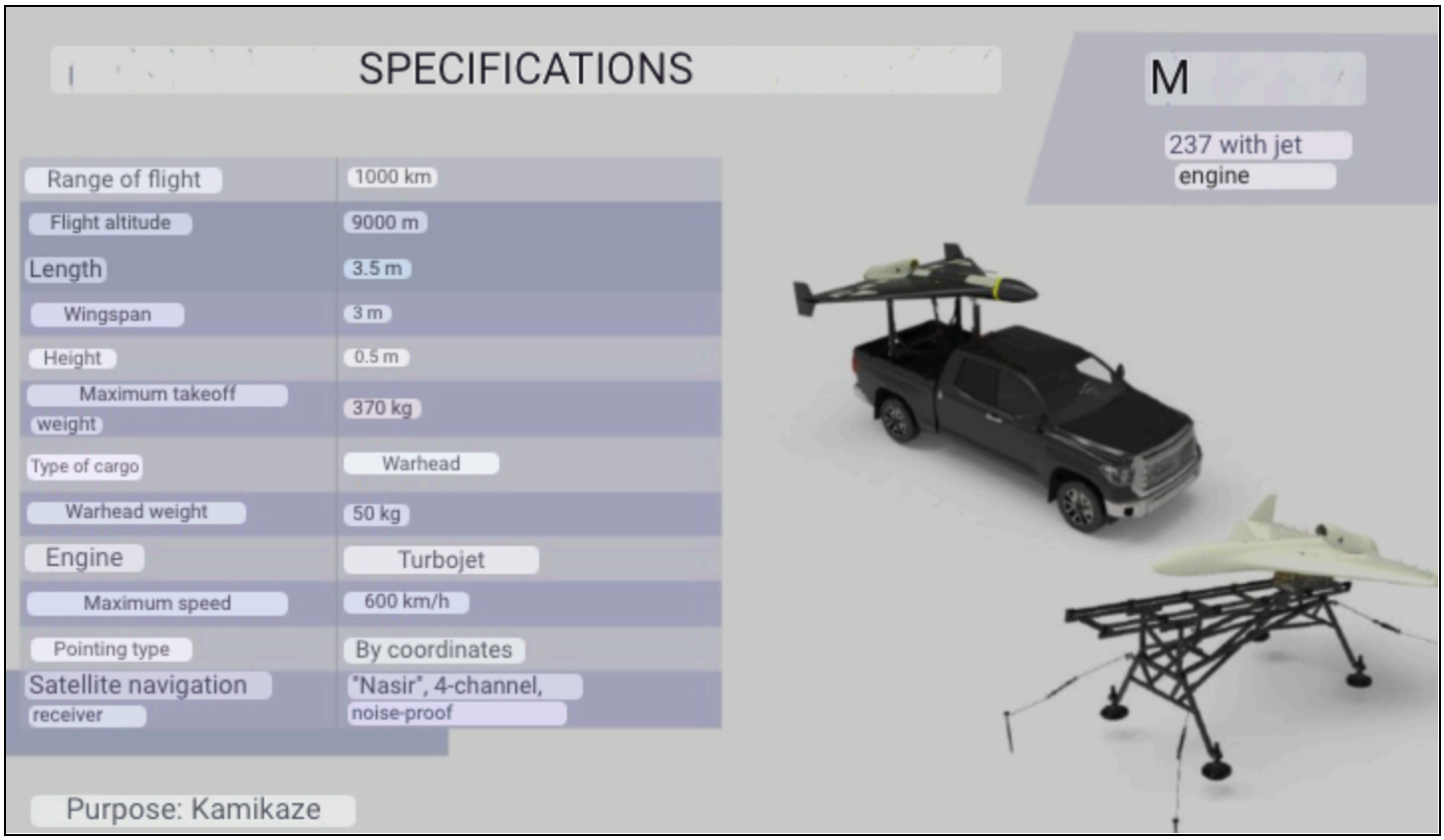


Figure 9: *Machine-translated version of a Russian-language document from an alleged hack of an IRGC-affiliated company showing specifications of the Iranian Shahed-238 drone, known in Russia as the M237 (Source: War Intel)*

The production contract's total price — including the technology transfer, equipment, 6,000 drones, and software — amounted to approximately $1.75 billion. According to the documents, Iran lowered its price from $375,000 to $193,000 per Shahed-136 drone for an order of 6,000 — a price that is significantly higher than Western experts had previously estimated each drone cost to produce. Russia also made some payments to Iran in gold ingots. The leaked documents, which US intelligence agencies have examined and whose authenticity they "do not dispute", underscore the substantial financial benefits Iran is reaping from its transfer of drone technology to Russia. Given the technological advances and economic boon that its drone partnership has delivered, Iran is almost certainly seeking to bolster its cooperation with Russia in this field. The earnings from drone sales help Tehran offset its trade imbalance — an estimated $16.8 billion non-oil trade deficit in 2023[11] — and decrease the economic isolation Iran faces as a result of global sanctions.

[11] *https://irannewsupdate[.]com/news/news-digest/irans-non-oil-trade-shows-deficit-in-2023/*

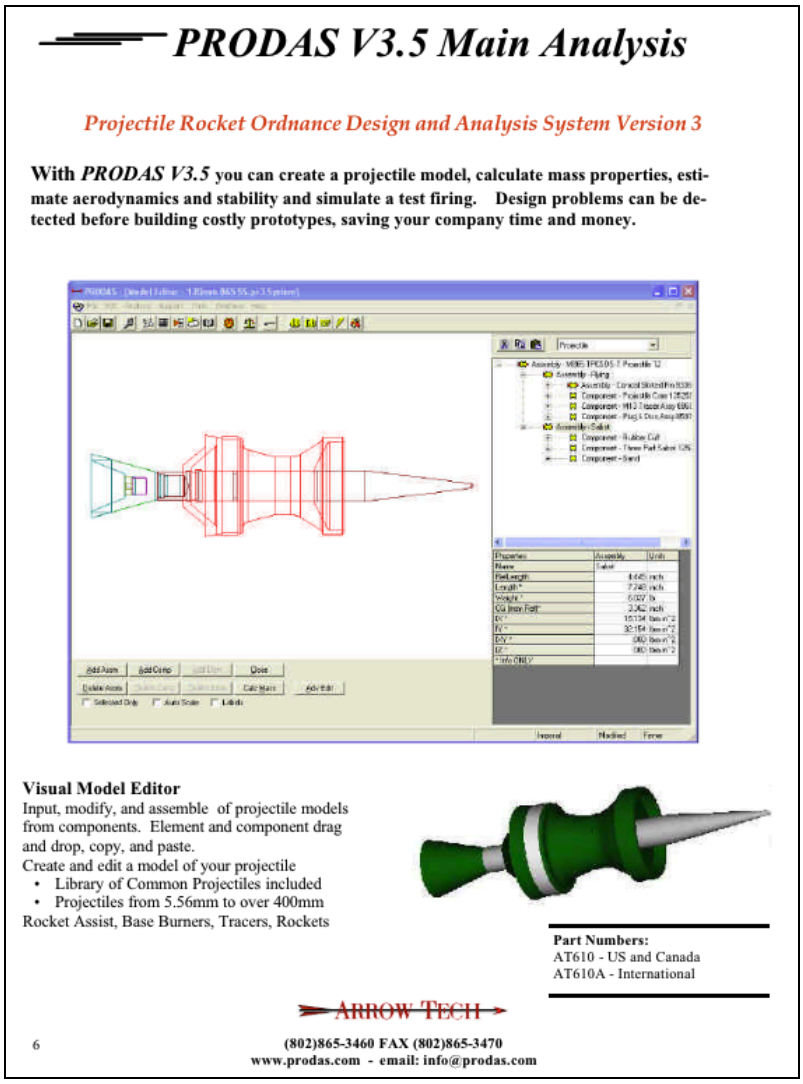
Cybersecurity Risk: Iranian Cyber Threat Actors Targeting Aerospace-Related Technology or Software

Iranian advanced persistent threat (APT) groups associated with the IRGC are likely seeking to leverage cyber-espionage capabilities to advance the design and production of advanced weapons, including drones. The aerospace technology industry has emerged as a frequent target for Iranian cyberattacks and will likely continue to be as the regime uses cyber tactics to complement its indigenous development and reverse-engineering efforts. Insikt Group assesses that the US, European, and Israeli defense industries — specifically, cleared contractors supporting military or intelligence programs involved in developing, testing, or producing drones, drone components or electronics, counter-unmanned aerial systems, or other related hardware or software — are likely at increased risk for Iranian cyber targeting. The following cyberattacks reflect the type of risk that Iranian threat actors pose to defense and aerospace industries.

Case Study: Iranian Hack of Arrow Tech Enabled Sale of Aerodynamics Analysis Software

In 2017, the US Department of Justice indicted two Iranian nationals, Mohammad Reza Rezakhah and Mohammad Saeed Ajily, for hacking a Vermont-based engineering and software design company, Arrow Tech. The company's main product — controlled by ITAR — was aerodynamics analysis and projectile design software called "Projectile Rocket Ordnance Design and Analysis System" (PRODAS). Ajily, associated with an Iranian software sales company, reportedly hired Rezakhah, a hacker with expertise in cracking encryption, to steal Arrow Tech's software. Rezakhah allegedly targeted Arrow Tech's computers and obtained unauthorized access to at least one of the company's computers in Vermont using Canadian and Dutch servers to hack into the networks. Ajily then transferred the PRODAS software to an unknown server location and onto Iranian computers.

Following Rezakhah's acquisition of the software, Ajily offered to sell the software to Iranian clients, including Iranian government entities and research centers known to specifically support Iran's drone technology development — namely, Sharif University of Technology — as well as other known MODAFL-linked institutions. Ajily received certificates of appreciation for his work from several Iranian government and military entities. Although this software theft was not drone-specific, it is likely that Iran would endeavor to target drone designs, software, or other technical information that could advance its drone development.



PRODAS V3.5 Main Analysis

Projectile Rocket Ordnance Design and Analysis System Version 3

With *PRODAS V3.5* you can create a projectile model, calculate mass properties, estimate aerodynamics and stability and simulate a test firing. Design problems can be detected before building costly prototypes, saving your company time and money.

Visual Model Editor
Input, modify, and assemble of projectile models from components. Element and component drag and drop, copy, and paste.
Create and edit a model of your projectile
- Library of Common Projectiles included
- Projectiles from 5.56mm to over 400mm

Rocket Assist, Base Burners, Tracers, Rockets

Part Numbers:
AT610 - US and Canada
AT610A - International

ARROW TECH

6

(802)865-3460 FAX (802)865-3470
www.prodas.com - email: info@prodas.com

Figure 10: *Arrow Tech's software catalog with details on its PRODAS V3.5 software, which was stolen and sold to the Iranian military (Source: Arrow Tech)*

Case Study: Mahak Rayan Afraz Targeting US Defense Contractor

In April 2024, the US Department of Justice revealed details about a multi-year cyber campaign targeting defense-related information conducted by four Iranian nationals — one of whom was directly linked to an IRGC cyber entity, the Organization for Electronic Warfare and Cyber Defense (IRGC EWCD). From 2016 to 2021, the four suspects used Iran-based company Mahak Rayan Afraz as a front to conduct a series of spearphishing operations under the guise of providing cybersecurity services. The group primarily targeted cleared US defense contractors that had access to classified information in support of US Department of Defense programs; it also hacked a New York-based accounting firm, compromising more than 200,000 employee accounts. In one attack, the group gained access to a US defense contractor's administrator account, allowing the conspirators to create unauthorized accounts that were then used to send spearphishing emails to employees of a different defense contractor and a consulting firm, attempting to gain unauthorized access to the computer systems of those two

additional companies. The group also used social engineering techniques of impersonating women to gain victims' confidence and then deploy malware onto their computers.

Figure 11: *US Department of State Rewards for Justice announcement for three Iranian hackers involved in targeting US-cleared defense contractors (Source: Rewards for Justice)*

The indictment does not indicate the targeted companies were specifically involved in programs related to drone technology, and it does not name which US defense contractors were victims of the hacking operations. However, this incident further demonstrates the type of cyber threat posed by IRGC-backed contractors supporting Iran's cyber espionage, which almost certainly poses a threat to Western drone-related defense contractors or software or component manufacturers.

Mitigations

The Iranian drone industry poses a myriad of threats to both businesses and governments related to compliance failure, reputational damage, Western technology cloning, global proliferation of deadly drone designs, and cyber-espionage attacks. The following mitigation strategies and actions offer ways that businesses can limit their exposure to these threats. We also highlight recommendations for how Western-allied governments can bolster efforts to combat the growing threat of Iranian drone proliferation and cyber espionage against Western countries' drone industries.

Businesses

- Establish and maintain robust compliance programs with preventive procedures, including risk assessments, internal controls, training, auditing, and testing. Ensure employees are aware of appropriate communications channels and are encouraged to report suspicious activity inconsistent with industry norms, and ensure efficient compliance review mechanisms are in place to enable timely disclosures to appropriate government authorities.
- Stay apprised of updated lists related to sanctioned persons or entities, those in violation of applicable export control laws, or end-user entities deemed a national security concern. Screen current and new customers, contractors, and intermediaries accordingly.
- Understand the various "red flag" methods that Iran and its foreign networks use to obtain drone components and technology, and practice customer due diligence policies outlined by relevant authorities, such as the US Departments of Treasury, Commerce, Justice, and State.
- Review updates to compliance policies of relevant export control regulatory bodies, and specifically be alert to the types of technology, componentry, or materials that are included in prohibited or controlled lists related to Iran's drone program. For example, on April 18, 2024, the US Department of Commerce imposed additional controls to further restrict Iran's access to low-level technologies that could be used in Iranian drones.
- Require completed end-user certificates and shipping documentation for foreign transactions to ensure an accurate understanding of purchases and shipments, and exercise vigilance in reviewing that documentation with the understanding that bills of lading, certificates of origin, invoices, and packing lists are frequently falsified.
- Prioritize cybersecurity mitigation strategies and best practices, adhering to guidelines such as those recommended by the US National Security Agency.
- Identify and eliminate cyberattack paths and vulnerabilities related to privileged access user accounts, and reduce opportunities for Iranian cyber targeting by mandating employees' online operational security vigilance and encouraging employees to avoid revealing specifics about their employers' programs or technology in professional and personal social media profiles.
- Implement an insider threat program, under a framework such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to deter, detect, and mitigate risk of exploitation, compromise, or unauthorized disclosure of sensitive drone-related technology.

- Use the Recorded Future Threat Intelligence Cloud to monitor and detect Iranian APT activity, maintain awareness of Iranian tactics, techniques, and procedures, and mitigate attack surface exposures and vulnerabilities commonly exploited by Iranian APT groups.

Government

- Enhance governments' analytic capabilities and resources dedicated to identifying Iranian illicit activities, transactions, companies, and networks supporting its drone program.
- Apply sanctions pressure to specialized production companies in Iran, and expand secondary sanctions targeting companies or entities in third-country facilitation hubs.
- Focus on controlling high-end, specialized components identified as critical for advancements in Iran's drone capabilities and inventory, such as satellite-enabled data links, advanced sensors, jet engines, electronic warfare equipment, and stealth or swarming technologies.
- Align US, UK, and EU approaches to "economic statecraft" through greater strategy coordination and increased information sharing, and ensure consistent enforcement of sanctions and export control frameworks.
- Address China's role as a key transshipment hub for drone parts to Iran, including through sanctions pressure on Chinese distributors and increasing Western manufacturing companies' awareness of compliance risks associated with Chinese trade companies.
- Increase cybersecurity collaboration and government-industry coordination across the defense sector, particularly cleared contractors involved in drone development or technology, through frameworks such as the US Department of Defense's Defense Industrial Base Cybersecurity Strategy.
- Use the Recorded Future Threat Intelligence Cloud to monitor and detect Iranian APT activity, maintain awareness of Iranian tactics, techniques, and procedures, and mitigate attack surface exposures and vulnerabilities commonly exploited by Iranian APT groups.

Outlook

Iran has derived significant strategic, economic, and regional military power projection benefits from building its drone industry, and Tehran is almost certainly committed to expanding it as a result of those benefits. Iran will almost certainly continue to bolster its domestic production capabilities and showcase its advances in indigenous manufacturing for domestic propaganda and foreign export purposes. Iran will almost certainly seek increased operational range and greater missile payloads, as well as pursue a number of technological improvements to its drone fleet, including jet-powered engines, electro-optical seekers, and satellite-enabled communications.[12] [13]

Iran will continue to expand its foreign engagement (drone diplomacy). Specifically, Tehran will almost certainly seek to strengthen its "unprecedented" strategic partnership with Russia through its joint

[12] During Iran's August 2023 Defense Industry Day — a showcase of achievements in Iran's defense sector — Iran's defense minister Ashtiani touted the Ministry's "drone leap" program, which was "actively pursuing the creation of the fifth generation of drones in the drone industry" and developing "artificial intelligence, electronic warfare, and signal collections".
[13] *https://www.tehrantimes[.]com/news/488232/The-lengthening-of-Iran-s-drone-arm*

drone manufacturing project, while exploring how to trade in other military systems. As Iran's April 13, 2024, direct attack on Israel has raised the risk of open warfare, Iran is almost certainly seeking to improve its own capabilities, specifically its air defense systems and advanced fighter jets, with the help of Russian military assistance. While Iranian drones may not have proven effective against Israeli and Western air defense capabilities, Iran's ability to produce drones at a lower cost than other types of aerial systems, such as missiles, will likely fuel foreign interest and demand in its drone program. To capitalize on the economic potential of expanding its drone sales, Iran will likely promote its potential exports to global customers in markets with anti-West, non-aligned, or war-torn countries, where international sanctions carry little weight. In addition to China, Iran will likely seek to identify additional hubs where sanctions are not recognized or enforced, such as Malaysia and Türkiye. The resilience of these foreign procurement networks will continue to challenge the compliance frameworks established by Western governments.

The factors driving Iran's continued expansion of its drone program will very likely continue to create risks over the long term. Iran's desired access to Western or Israeli technology will likely continue to factor into Iran's offensive cyber operations, driving cyber-espionage risk for Western defense industries. Iran's pursuit of electronic warfare capabilities to capture Western or Israeli drones, combined with its reverse engineering industry, poses an ongoing threat of technology transfer. At the same time, Iran is unlikely to give up its reliance on Western-made components, and Iran will likely continue to apply its years of sanction evasion experience by establishing new cover companies, procurement networks, alternative payment mechanisms, and sourcing processes to obtain Western-made components it cannot replicate domestically.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com