THREAT ANALYSIS

IRAN

Recorded Future®

Insikt Group®

July 16, 2026

AI Has Enhanced Iran's Asymmetric Playbook During the 2026 Conflict

AI has almost certainly enhanced Iran's cyber, influence, targeting, and surveillance capabilities, but has not fundamentally altered the asymmetric doctrine underpinning Iran's conflict strategy.

Iran will likely continue integrating AI into its cyber and influence operations to strengthen narrative credibility and accelerate the development and deployment of digital threats.

Iran-Russia drone cooperation will likely remain a threat, as Iran stands to benefit from Russia's AI-enabled drone advances and tactical experience in Ukraine.

Executive Summary

Between January and June 2026, Tehran survived unprecedented military, economic, and political pressure by relying on its longstanding hybrid warfare model: blending asymmetric military operations, cyber operations, information warfare, proxy attacks, and coercive state control. Artificial intelligence (AI) enhanced these capabilities, acting as a force multiplier and almost certainly increasing the speed, scale, and effectiveness of Iranian operations. Ultimately, Iran demonstrated that its strategic resilience does not depend on possessing the most advanced AI capabilities; rather, the source of Iranian power remains the asymmetric playbook itself.

During these crises, Iran compensated for conventional military and economic disadvantages through scalable, low-cost, and deniable asymmetric capabilities. Iran's use of AI almost certainly improved its cyber capabilities, accelerated the production of propaganda and influence narratives, and expanded the reach of information campaigns. AI's impact on Iranian military operations is less clear, as Iran's battlefield use of AI has not been independently confirmed. However, the support Russia provided to Iranian military operations increases the likelihood that AI-enabled tactics and capabilities, refined in Ukraine, contributed to Iranian drone attacks against Israel and Persian Gulf states. Domestically, AI-driven surveillance systems deployed during and after the 2022 "Woman, Life, Freedom" protests likely facilitated the Iranian regime's violent suppression of unrest in January 2026.

As low-level conflict persists and the risk of a return to war with the United States (US) and Israel remains heightened, Iran's expanding use of AI-enabled cyber operations will likely pose an elevated threat to Western and regional critical infrastructure and vital industries. Iran's rapid production and dissemination of AI-generated propaganda expose corporate and state entities to highly targeted influence operations (IOs), risking erosion of customer and citizen trust. As Iran rebuilds its military arsenal, its acquisition of Russian-backed drone capabilities will pose an ongoing risk to critical infrastructure and maritime logistics in the region. Across all sectors, Iran's hybrid warfare capabilities will likely continue to pose a risk to digital and physical assets, requiring organizations to build resilience against AI-enhanced asymmetric threats that are more scalable and harder to attribute.

Key Findings

- In 2026, AI technologies very likely accelerated existing Iranian capabilities across cyber, influence, military, and domestic repression domains, rather than creating new ones.
- AI's clearest strategic impact for Iran has been in its information warfare, as AI content generation enables Iran to shape perceptions of the conflict by rapidly producing widely resonant propaganda and influence content.
- Iran's AI advances appear tied to foreign partnerships — Russian military AI and drone innovations, as well as Russian and Chinese surveillance technologies; Tehran will likely seek to incorporate these foreign AI innovations into its established playbook.
- Organizations and governments should strengthen defenses against AI-enhanced Iranian tradecraft — including AI-assisted phishing, cyber intrusions targeting operational technology, and IO campaigns — while ensuring resilience against combined cyber and physical disruption efforts.
- Post-conflict, Iran is likely to prioritize rebuilding the missile, drone, and maritime capabilities that underpin its asymmetric deterrence model while integrating AI, where possible, to improve efficiency and effectiveness.

Table of Contents

Background **4**
AI Enhancing Iran's Asymmetric Capabilities **4**
Cyber Operations 4
Reconnaissance and Operational Research 4
Code Writing and Malware Development 5
Social Engineering and Phishing Operations 6
Deniability 7
Influence Operations 8
Stoking Anti-US, Anti-Israel, and Pro-Regime Sentiment 8
Promoting False Information to Project Regime Strength 10
Inflating Military Effectiveness 10
Fabricating Regime Support 12
Automated Propagation Through Inauthentic Accounts 13
Military and Intelligence Operations 13
AI in Russian Drones Raises Potential for Technology and Tactics Transfer to Iran 14
AI in Indigenous Iranian Drones 16
AI in Iranian Missiles 17
AI in Iranian Naval Operations 18
Domestic Security 18
FindFace 18
Surveillance Infrastructure 19
Mitigations **20**
Outlook **20**

Background

Following a directive issued by former Supreme Leader Ali Khamenei in 2021, Iran pursued a centralized national AI strategy intended to expand domestic research and development, reduce technological dependence on foreign actors, and position the country as a regional technological power. However, Tehran's AI ambitions have faced severe economic constraints and technological limitations as a result of sanctions and isolation.

Between the 2021 directive and the 2026 conflicts, Tehran prioritized developing AI for use in cyber operations, influence campaigns, intelligence and military systems, and domestic repression. Iranian threat actors incorporated generative AI and large language models (LLMs) into spearphishing, social engineering, and online IOs, while Iranian officials publicly emphasized AI-enabled drone, missile, and intelligence capabilities. More broadly, Iran appears to view AI not only as an economic and technological imperative, but also as a tool for preserving regime security and offsetting the strategic constraints imposed by its international isolation.

AI Enhancing Iran's Asymmetric Capabilities

Insikt Group analyzed cybersecurity and AI threat reports, social media, Iranian state-run messaging and government/military statements, and activist investigations to illuminate Iran's AI use, or lack thereof, during 2026. While Iran's unprecedented internet blackouts create significant gaps in open-source understanding of Iran's AI capabilities during domestic crises and wartime, one theme is clear: AI has almost certainly enhanced Iran's asymmetric tactics and hybrid warfare doctrine, but has not fundamentally altered the strategic logic underpinning Iran's approach to the conflict.

Cyber Operations

Iran's use of AI to support the cyber dimension of its conflict with the US and Israel predates the January 2026 protest crackdown and the February 28, 2026, coordinated US-Israeli airstrikes, known as Operation Epic Fury / Roaring Lion. The 2026 crises likely prompted Iranian state-sponsored and state-aligned threat actors to leverage generative AI to gain productivity and tradecraft improvements across reconnaissance, code/malware development, social engineering, and translation. However, AI has not fundamentally shifted Iranian cyber capability. Iran's 2026 campaign has remained anchored in the same baseline TTPs — including spearphishing, wiper malware, credential theft, abuse of legitimate enterprise tooling, and hack-and-leak operations — that pre-date the AI era. The pattern is consistent with what Google, OpenAI, and other AI developers have documented since 2024: AI accelerates and scales what Iranian actors were already doing, rather than enabling new capabilities.

Reconnaissance and Operational Research

In October 2024, OpenAI reported that Iran-linked hacktivist persona "CyberAv3ngers" used ChatGPT to conduct reconnaissance on programmable logic controllers (PLCs), a use case that has continued to

bolster Iranian capabilities against industrial control systems (ICS) during 2026. According to CloudSEK, AI is accelerating the research phase in ICS attacks: "An actor can move from intent to a list of accessible US ICS devices with known default credentials in under five minutes." CloudSEK researchers recreated CyberAv3ngers's research on vulnerable US-based ICS systems in an unspecified AI LLM agent and identified an additional exposed ICS portal, highlighting a critical infrastructure "playbook that other groups can now replicate much more easily with the help of AI." Using this research playbook, Iranian threat actors can not only identify vulnerable ICS systems but also understand the unique properties of the specific technologies they are targeting.

In May 2026, an attack attributed to "Cyber Isnaad Front" targeted an Israeli industrial refrigeration system, sabotaging the system by programming it to fail. While there is no direct evidence of AI use in this incident, the attack required expertise in both Windows internal coding and refrigerant physics to ensure maximum damage, suggesting in-depth research into the target system. The targeting selection demonstrates that Islamic Revolutionary Guard Corps (IRGC)-backed cyber personas are concentrated on identifying vulnerabilities in adversaries' supply chains, logistics, industrial operations, and food production. By facilitating research, AI lowers the level of expertise required to target ICS systems across multiple critical industries.

Code Writing and Malware Development

Iranian-linked threat actor groups also use AI to accelerate their malware development capabilities. In February 2026, Google's GTIG AI Threat Tracker reported that GreenBravo (also known as APT42, Charming Kitten, Mint Sandstorm) has been using Gemini "as an engineering platform to accelerate the development of specialized malicious tools," including for debugging, code generation, and researching exploitation techniques. Another example is Operation Olalampo, first observed on January 26, 2026, and attributed to GreenGolf (also known as MuddyWater, Mango Sandstorm) in a Group-IB report. The campaign delivered four novel malware families (CHAR, GhostFetch, GhostBackDoor, HTTP_VIP) against MENA targets via spearphishing. Group-IB's analysis of the Rust-based CHAR backdoor identified debug strings containing emojis — "a trait rarely seen in human-authored code" — across four separate instances. Group-IB assessed that the emojis indicate the operator used an AI model to generate code segments and failed to sanitize debug strings before compilation. Group-IB explicitly tied this to Google's earlier reporting that MuddyWater was already experimenting with Gemini for file transfer and remote execution code.

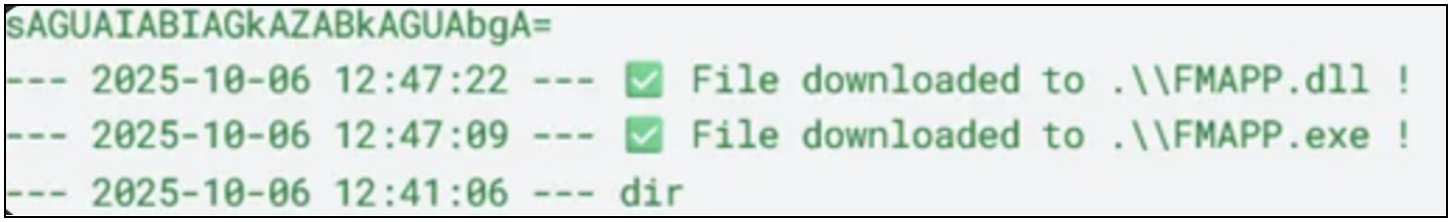

Figure 1: *Emojis used in CHAR malware suggest AI use (Source: Group-IB)*

In January 2026, HarfangLab reported on a newly identified threat actor dubbed RedKitten, targeting Iranian non-governmental organizations and human rights activists during the January 2026 protests. The campaign used malicious Excel files purportedly listing protesters killed during the regime crackdown between December 22, 2025, and January 20, 2026. The files, presented as forensic medical records but assessed to contain fabricated data, deployed a C# implant when opened. HarfangLab noted similarities to IRGC-aligned Imperial Kitten tradecraft, particularly the targeting of domestic dissidents through weaponized documents. The firm also assessed with confidence that the actor "rapidly built this campaign using AI tools, as indicated by multiple traces of LLM-assisted development" in both the VBA macro and the implant. Notably, HarfangLab concluded that AI assistance "could not compensate for an apparent hasty integration and lack of deep technical understanding" — a useful indication that AI can accelerate malware development but does not yet replace skilled operators. Similarly, ZScaler ThreatLabz observed several "fingerprints" of generative AI in the TWINTALK and GHOSTFORM malware used by Iran-linked threat actor Dust Specter (who overlaps with the APT34 subcluster tracked as TAG-135) against Iraq's Ministry of Foreign Affairs, including telltale emojis and Unicode text in the codebase.

During the Iran War, IRGC-affiliated Nimbus Manticore reportedly used malicious lures impersonating organizations in the aviation and software sectors across the US, Europe, and the Middle East. Researchers at Check Point assessed that the threat actors leveraged "LLM-based tools and AI-assisted development techniques" during the malware creation. Check Point based its assessment on "multiple indicators" of AI use in the MiniFast backdoor's coding patterns and operational implementation. Additionally, Ababil of Minab, a new hacktivist persona likely tied to Iran's Ministry of Intelligence and Security (MOIS), reportedly used ChatGPT to refine the script used to enumerate and drop databases in an April 11 cyberattack targeting Vyncs, a US-based consumer GPS vehicle-tracking service. Earlier in the conflict, Ababil of Minab claimed responsibility for disruptive attacks on the Los Angeles Metro, South Florida Regional Transportation Authority (SFRTA), and UNIMAC (United Maintenance and Contracting Company), which is based in Saudi Arabia.

Social Engineering and Phishing Operations

Iranian state-sponsored hacking groups continue to use AI to enhance their social engineering and phishing lures. GTIG's February 2026 report found that APT42 supplied Gemini with a target's biography and used it to "craft a good persona or scenario to get engagement from the target." Google labels this workflow "rapport-building phishing," where the attackers earn trust through "multi-turn, believable conversations" with victims before delivering the payload. Google more broadly observed that LLMs are now used to "generate hyper-personalized, culturally nuanced lures that can mirror the professional tone of a target organization or local language," making the lures more likely to deceive the victim.

The use of LLMs has likely enhanced Iran's ability to create highly convincing content through foreign-language translation, enabling greater fluency and increasingly rapid generation of conflict-themed phishing lures that exploit current events. Iran has used AI since at least late 2024 for these use cases: OpenAI's October 2024 disclosure revealed Storm-0817 using ChatGPT to translate LinkedIn profiles into Persian to support targeting work, and Educated Manticore (overlaps with

GreenBravo, APT42, Charming Kitten, Mint Sandstorm) used AI tools to craft email and WhatsApp messages to target Israeli technology and cybersecurity experts in June 2025. In 2026, phishing emails targeting Gulf countries surged by nearly 130%, according to Bitdefender, with cyberattacks targeting the UAE doubling in March. Iran-aligned actors are very likely leveraging AI-generated content to exploit conflict-related themes and security update pretexts in phishing lures tied to kinetic events. For example, Iran-linked actors have deployed a campaign involving a malicious replica of the Israeli Home Front Command Red Alert application. APT34 (aka TA402, OilRig) reportedly used compromised Iraqi Ministry of Foreign Affairs infrastructure — the same used by the Dust Specter cluster mentioned above — to target a Middle Eastern government using lures referencing "potential US ground operation in Iran" and "Gulf military alliance." In the domestic sphere, digital rights advocacy group Filterbaan reported on a voice-message lure operation impersonating a senior Iran International executive, warning that AI-produced voices pose a threat to activists.

Figure 2: *Screenshot of WhatsApp conversation targeting an Iranian activist using an AI voice impersonation (Source: Social media)*

Deniability

The use of AI agents will likely enable Iranian cyber intrusion and espionage groups to maintain plausible deniability and challenge TTP-based attribution, as automation of key elements of a cyber operation lifecycle can obscure the patterns and operational behaviors that are used to establish a link to known threat actors. Generative AI is likely to facilitate deniability by enabling the scalable creation of personas, narratives, and supporting content that can obscure state involvement. AI tooling also strips out many of the behavioral fingerprints on which attribution has historically depended: a 2025

peer-reviewed analysis of generative AI in cybersecurity notes that "behavioral patterns for attribution, such as code similarity, compilation timestamps, working weeks, holidays, and language, could disappear when GenAI creates Offensive Cyber Operations (OCO) code." Iranian APT groups have used this AI-driven obfuscation to "complicate forensic investigations," "hinder intelligence-sharing efforts," and "reduce the effectiveness of traditional attribution methodologies."

Influence Operations

AI's greatest utility for Iran since the start of 2026 has very likely been in augmenting its information warfare. From the January 2026 protest crackdown through the post–February 28 conflict with the US and Israel, both pro-Iran influence networks and state-backed media have exploited AI-generated content to serve a strategic set of objectives: stoking anti-US, anti-Israel, and pro-regime sentiment; projecting military strength and exaggerating battlefield impact; and automating content propagation through inauthentic accounts. In the influence operations domain, the most consequential element of Iran's use of AI is not any single fake video but Iran's aggregate ability to flood the global information environment with synthetic content at a speed and scale that has fundamentally outpaced platform moderation, attribution research, and counter-messaging. Whereas AI has streamlined specific elements of Iranian cyber operations, it is enhancing IOs by boosting production tempo, visual and audio polish, and cultural reach.

Stoking Anti-US, Anti-Israel, and Pro-Regime Sentiment

Iran's most recognizable AI-driven information product of 2026 has been the "Lego" series of propaganda videos, produced by "Explosive Media," formerly "Akhbar Enfejari," (@ExplosiveMediaa, formerly @Akhbarenfejari) account. The group claims to be independent and student-run, but a representative of Explosive Media confirmed to the BBC that the Iranian regime is a "customer." The anti-US videos include Lego-character versions of US President Donald Trump and Israeli Prime Minister Benjamin Netanyahu, and reference politically sensitive US topics, such as the Jeffrey Epstein files and the death of George Floyd. The videos' narratives fuse mockery of Trump and his administration, acts of vengeance against the US, and solidarity with Iranian and other populations perceived as victimized by the US. According to a representative of Explosive Media interviewed by the New Yorker, AI enables the group to produce a two-minute video in about 24 hours, and the rap songs that accompany the videos use an AI-generated voice.

Figure 3: *Screenshot of a Lego video portraying President Trump, with Prime Minister Netanyahu, initiating a strike on an elementary school in Minab, Iran, on March 10, 2026 (Source: Social media)*

In a similar thematic narrative, Iranian diplomatic accounts published a series of AI-generated content exploiting American pop culture references and Western iconography in provocative memes. The posts are often trolling attacks that are intended to directly humiliate US leadership figures, such as a video of Jesus slapping President Trump after Trump posted a controversial image of himself as Jesus. An Institute for Strategic Dialogue analysis found these accounts generated nearly one billion views in 50 days and 22 million likes — 30 times their prewar baseline. AI almost certainly enhanced Iran's ability to quickly and effectively produce content with themes that resonate with both its own population and an international audience, particularly tailored to a younger generation that has global cultural exposure.

If the Lego videos and Trump trolling are aimed at portraying a weak US administration, Iran has also exploited AI to legitimize its own regime. A prominent example is Iranian state media's circulation of an AI-generated, Japanese anime-style video titled "Khamenei Is Back," depicting the senior Khamenei in the moments before his death; his son Mojtaba finds the deceased leader's ring in the rubble and assumes the leadership role, directing a barrage of missiles at Washington. Mojtaba Khamenei was reportedly injured in the strike that killed his father and has not been seen or heard from publicly since; nevertheless, the AI-enabled visual depiction of the new Supreme Leader as a powerful figure carrying on his father's legacy presented a legitimizing narrative to offset Mojtaba's absence from public view.

A Note on Attribution

Attribution of AI video, image, or content production to the Iranian state for the most viral AI content outlined here remains uncertain. The strongest documented links to Iran's security apparatus are the publishing and amplification of content by state outlets. In the case of the Lego series, videos have been redistributed almost in real time by IRGC-controlled Tasnim News and other state-aligned outlets. Some Western media have also pointed to an apparent Revayat-e Fath (Persian: روایت فتح) watermark on early-release videos as indicative of a link to the Revayat-e Fath Foundation, an IRGC-affiliated cultural center that produces cinematic features about Iranian military engagements. An Explosive News representative denied the link, saying that Revayat-e Fath, meaning "Chronicles of Victory," was simply the title of the first two videos. Despite a lack of evidence that the Iranian state is directly producing the content, the Iranian government very likely co-opts or contracts with private technology companies or collectives, such as Explosive Media, to support its information warfare themes and objectives. As such, the propaganda narratives are likely state-backed and approved, even if not state-produced.

Promoting False Information to Project Regime Strength

Inflating Military Effectiveness

Tehran has leveraged AI-generated images and videos throughout the conflict to inflate perceptions of its military effectiveness, portray the US and Israel as vulnerable, and distort domestic and global assessments of the war's impact. Within the first two weeks alone, AI-generated content falsely depicted Iranian missile strikes on Tel Aviv; panicked civilians fleeing a fabricated airport attack; captured US special forces; a US convoy operating inside Iran; a downed US aircraft paraded through Tehran; burning US facilities in the Gulf; and satellite imagery showing damage to a US base in Bahrain. Iranian state-affiliated media amplified claims of its military effectiveness by pairing them with AI-fabricated visual evidence of destroyed facilities. A prominent example came on March 1, when Iran claimed it had struck the USS Abraham Lincoln. At the same time, an AI-generated video circulated online showing the carrier ablaze with fighter jets falling into the sea, prompting a public rebuke from President Trump on the use of AI for disinformation. By flooding the information environment with realistic but false visuals, Tehran likely sought to strengthen its control over the wartime narrative by exaggerating its battlefield successes, shaping domestic perceptions of resilience, and influencing international coverage. Chinese and Russian information networks further amplified these narratives, such as the circulation of a fake image claiming the Iraqi resistance had shot down a US KC-135 aircraft in early March 2026. At the start of the conflict, a China-linked influence network began posting AI-generated content seeking to undermine the legitimacy of US strikes on Iran, highlight morale issues among the US armed forces, and amplify the potential economic fallout for US citizens as a consequence of the war.

Figure 4: *Screenshot of a false AI-generated video allegedly showing the USS Abraham Lincoln after an Iranian strike (Source: AFP)*

According to a Cyabra report, another Iranian IO campaign used AI to "fabricate and weaponize scenes of American casualties, suffering, and military failure." The analysis identified 47 inauthentic accounts generating over 40 million views of AI-generated content depicting three specific themes: US military funeral processions, deployed American soldiers in distress, and families mourning loss. Cyabra research suggests hundreds of videos were likely derived from only two or three underlying AI prompts, suggesting centralized, AI-driven production behind the appearance of grassroots authenticity. This campaign is aimed at magnifying the psychological toll of US losses and stoke public pressure to curtail US military operations against Iran.

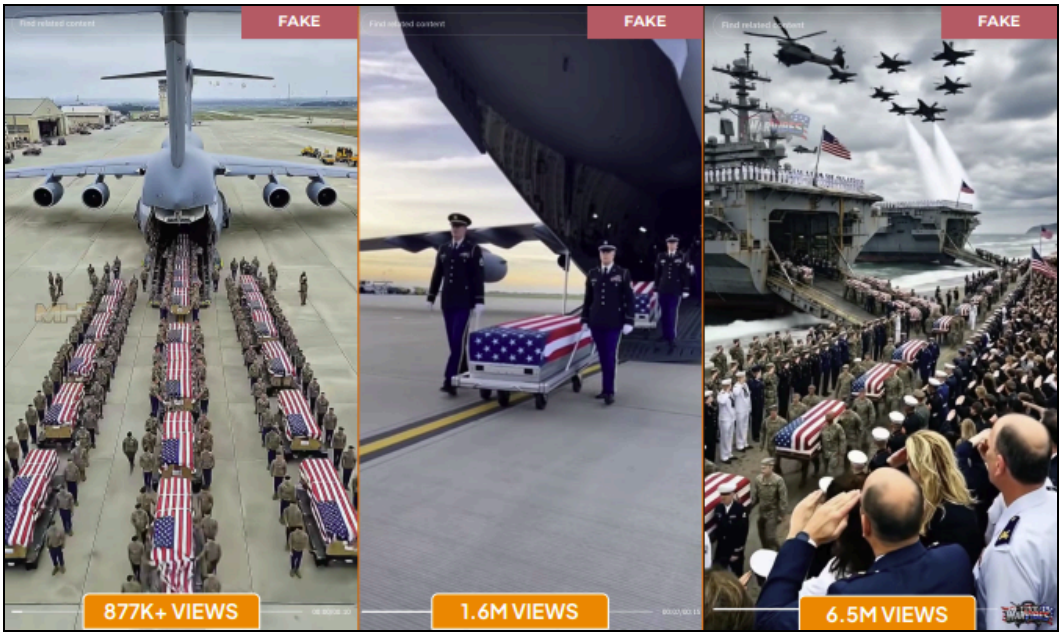

Figure 5: *AI-generated content depicting US military funeral processions (Source: Cyabra)*

Fabricating Regime Support

A separate but related strand of Iran's strength-projection AI use has been to manufacture the appearance of mass domestic support for the regime, first during the January 2026 protests and again during the wartime period since March. As anti-regime demonstrations spread across Iran in early January, AI-generated videos purporting to show enormous pro-government counter-rallies circulated widely on social media. In one example, Iranian state media aired a video allegedly showing crowds of regime supporters lining a massive Iranian flag, which was debunked as AI-generated, originating from a post that TikTok itself labeled as AI. However, the wartime crowd-size picture is muddied from both sides: Iran has demonstrably inflated pro-regime rally content with AI, but real and substantial pro-regime gatherings, including photojournalist-verified New York Times imagery from Tehran, have also been falsely dismissed as AI-generated. During the height of the protest period, AI-generated imagery depicting pro-regime themes circulated widely on social media, such as content portraying the US and Israel as instigators of the uprising and casting Crown Prince Reza Pahlavi as a pawn of Israel (**Figure 6**).

Figure 6: *Pro-regime AI-generated images circulated on social media blaming Israel and the US for the unrest (left), and portraying Crown Prince Pahlavi as Israel's pet (Source: Recorded Future)*

Automated Propagation Through Inauthentic Accounts

Beyond content creation, AI enables Iran to amplify narratives at scale through networks of fake personas that disseminate false information and propaganda. The use of AI to quickly generate and credibly backstop inauthentic accounts with images, activity, and content propagation has helped Tehran disseminate its messaging across platforms and geographies.

Storm-2035 is a prime example of such an amplification network, which remains operational despite a Meta takedown in early 2026. The multilingual network of social media, Instagram, and Bluesky accounts pivoted within 24 hours of the February 28 strikes from divisive Western political content (anti-United Kingdom monarchy, pro-Scottish independence) to overtly pro-regime messaging, such as an AI-generated image of a destroyed US base in the Middle East. The network operates a two-tier architecture of "creator" and "amplifier" in which the creator personas, described in Meta's reporting as having "well-developed backstories," use AI-generated profile pictures to increase their credibility; Insikt Group tied at least one persona's image to AI image generator platform *freepik[.]com*. The amplifier personas drive engagement through reactions, comments, and shares. OpenAI previously reported observing this network using ChatGPT to produce content in different languages, for different personas.

Attack Alarm is another case study of an information asset's overt repurposing. The Hebrew-language social media persona (@Attack_Alarm1) originally masqueraded as an Israeli missile-warning service during the June 2025 conflict; since the February 28 strikes, it has dropped that pretense entirely and surged in its promotion of pro-Iran narratives, including AI-generated content. The persona has shared AI-enabled images of Iranian missiles flying toward US and Israeli flags (with Epstein-themed captions), AI-generated images of the destruction of a US Terminal High Altitude Area Defense (THAAD) site in Al Ruwais, UAE, and an AI-generated image implying Netanyahu had been killed after canceling a state visit. The account has also served as the visible amplification node connecting hacker fronts to influence outputs, repackaging claims from Handala Hack Team, Cyber Av3ngers, and Cyber Isnaad Front.

Military and Intelligence Operations

In the months and years preceding the 2026 conflict with the US and Israel, Iranian media leadership consistently promoted the integration of AI capabilities across its drone, missile, and naval platforms. Some of the military systems Iran employed during the conflict were likely equipped with AI-enabled features and autonomous capabilities, which may have enhanced strike effectiveness in specific instances, but the extent to which AI contributed to the overall success of Iran's drone, missile, and maritime operations remains unclear based on publicly available reporting. Russia's reported sharing of drone technology with Iran and its documented use of AI in drone operations in Ukraine are likely the most plausible indicators of potential AI use in Iran's kinetic attacks.

However, AI does not appear to have been a decisive driver of Iran's operational successes. Iran's most significant military effects have largely relied on asymmetric tactics that predate the widespread

adoption of AI, such as sustained missile and drone campaigns targeting US bases and Gulf and Israeli civilian infrastructure, the disruption of maritime traffic through the Strait of Hormuz, and attacks against commercial shipping. These tactics have long been foundational elements of Iran's asymmetric doctrine: high-volume saturation attacks designed to overwhelm air defense systems; low-cost unmanned aerial and naval systems capable of swarm operations; and exploitation of Iran's unique strategic geography, which gives it direct access to a critical commercial chokepoint.

AI in Russian Drones Raises Potential for Technology and Tactics Transfer to Iran

Ukrainian Defence Intelligence (HUR) published evidence of AI integration in Iranian drones in June 2025, when Ukrainian air defense units intercepted what was initially assessed as a standard Iranian-made Shahed-136 over Sumy Oblast in northeast Ukraine. Upon technical exploitation, HUR specialists found it to be an upgraded "MS001" series variant that matched the description of a Shahed-236 in Russian documentation. The drone was equipped with an Nvidia Jetson Orin AI module paired with a thermal imaging camera, enabling autonomous target identification and terminal-phase guidance without reliance on GPS. Ukrainian Major General Vladyslav Klochkov characterized the new version of the Shahed drone platform as a "digital predator," with onboard technology enabling object recognition, thermal processing, and trajectory adjustment. This discovery revealed the integration of AI in an Iranian-designed platform, deployed by Russia against Ukraine.

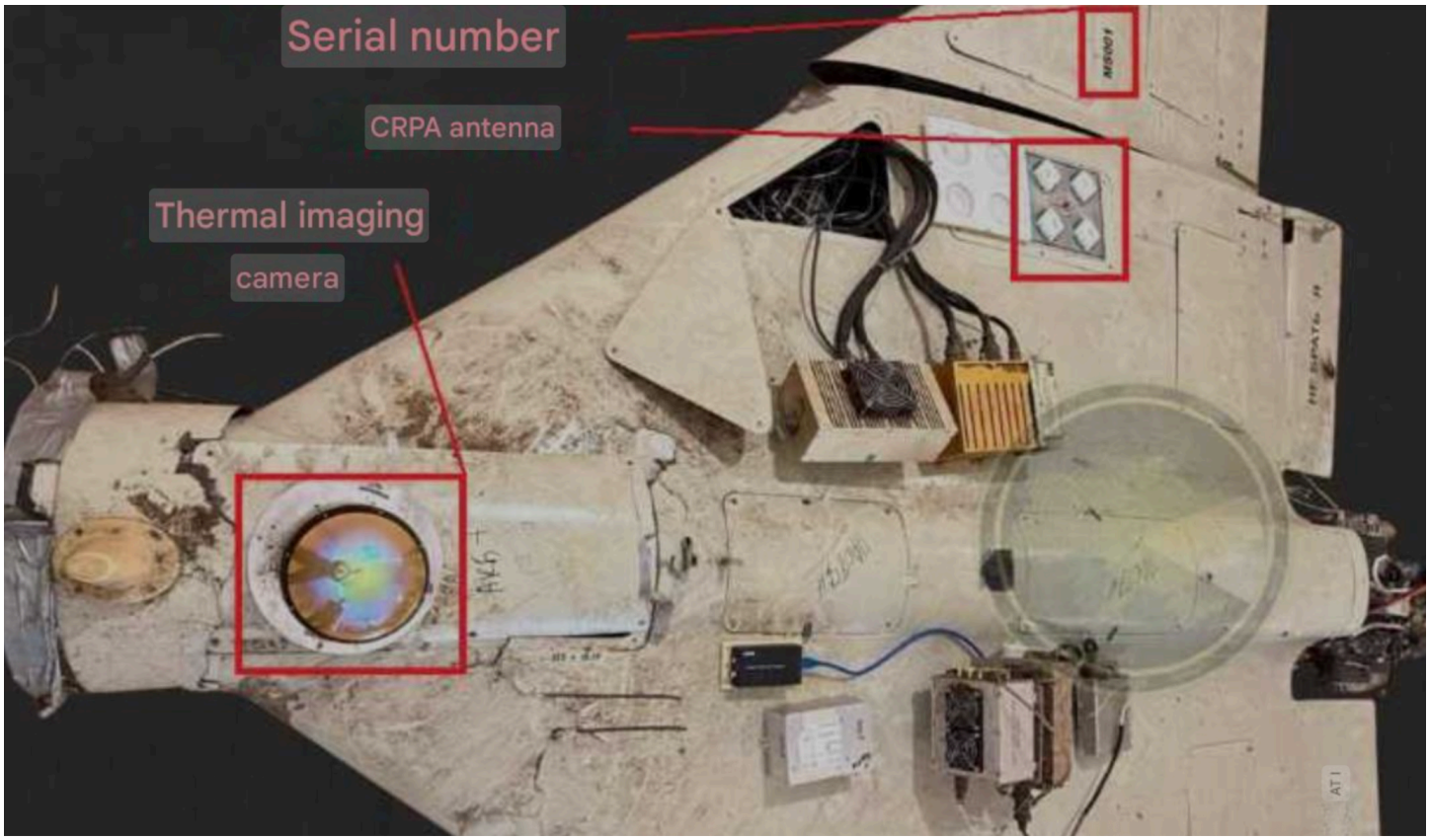

Figure 7: *Google-translated image showing wreckage of upgraded Shahed-236 (Russian MS001) drone with an Nvidia Jetson AI system (Source: Militarnyi)*

Insikt Group has not identified public evidence confirming that Iran deployed the same AI-enabled Shahed drone variants during its 2026 attacks on US, Gulf, or Israeli targets. Between February 28 and June 1, 2026, no publicly reported physical exploitation of downed Iranian drones has specifically identified AI components, autonomous modules, or other indicators comparable to those documented by HUR in Ukraine. UAE Defense Ministry spokesperson Brigadier General Abdul Nasser Al Humaidi revealed during a March 3 press briefing that the UAE's air defenses had neutralized hundreds of Shahed-136, Shahed-107, and Shahed-238 drones, without mentioning AI-enabled variants.

Nevertheless, multiple reports indicate ongoing transfers of advanced drone capabilities from Russia to Iran. Open-source analysts examining unconfirmed images posted of drone debris allegedly discovered near Dubai's Jebel Ali port on March 4, 2026, documented Geran-2 wreckage bearing the Cyrillic "KB" serial marking, indicating it was produced around 2024 at the Kupol plant in Izhevsk — suggesting Russia was supplying drone hardware used by Iran during the 2026 conflict. Western media reports reinforce this supply relationship: a US defense official briefed on the alleged transfer specifically raised the possibility that Moscow "might be providing Iran with other Shahed variants that are jet-propelled, use AI to pilot the drone even without a signal, or that are equipped with cameras for reconnaissance." In further evidence of the Russia-to-Iran drone supply, the Wall Street Journal reported that Russia provided components of "modified" Shahed drones, including technology to "improve communication, navigation and targeting." The Economist reported in early May 2026 on a confidential ten-page proposal indicating Russia had offered to provide Iran with "unjammable" drones, including fiber-optic and satellite-guided drones equipped with Starlink terminals, as well as training on how to use them in the early weeks of the war. Given that Russia demonstrably fielded AI-enabled Iranian-designed drones in Ukraine in 2025 and reportedly agreed to supply Iran with drone hardware during the 2026 conflict, it is plausible that the transferred drones may have included AI-capable variants, even if their operational use has not been independently verified.

A separate line of evidence also suggests that Russia may have transferred AI-enabled drone tactics and operational tradecraft to Iran. On April 29, 2026, Colonel Yuriy Cherevashenko, deputy commander of UAVs for air defense in the Ukrainian Air Force, identified Russia's use of artificial intelligence to generate "fresh approaches and flight plans" as one of the most significant adaptive challenges Ukraine faces, alongside drone "mesh networks" in which Shaheds act as signal repeaters for one another to defeat Ukrainian navigation jamming. These developments indicate that Russia's application of AI extends beyond onboard drone hardware and increasingly supports mission planning, route optimization, and coordinated deployment concepts. Separately, Russia reportedly shared "tactical guidance" with Iran to support its 2026 campaign against US and Gulf forces, according to the Wall Street Journal. Insikt Group has not identified open-source reporting confirming that Iranian drone attacks on the US, Gulf, and Israel used Russia's AI-enabled flight planning techniques. However, given Russia's alleged transfer of both drone hardware and operational know-how to Iran during the conflict, it is plausible that this cooperation extended to the AI-driven targeting and flight-planning tradecraft Russia has been actively developing and deploying against Ukraine. Even if some of Russia's efforts to integrate AI into drone operations remain aspirational or in development, rather than demonstrated

through deployments of fully autonomous capabilities in Ukraine, Russia-Iran cooperation on drone technology could support Iran's adoption of AI-enhanced drone tactics in the near future.

Figure 8: *Visual depiction of potential transfer of drone-related AI technology and tactics from Russia and its corresponding impact on Iranian drone operations (Source: Recorded Future[1])*

AI in Indigenous Iranian Drones

Iran claims to have integrated AI capabilities into its latest Shahed variant, which it may have used during the 2026 conflict. In November 2025, Iranian media reported on the IRGC's Shahed-161 drone, which Iran describes as a "stealth" drone featuring AI-enabled targeting and coordination. State-run PressTV described the new system as symbolizing "Iran's leap in indigenous defense tech" that showcases "advanced stealth and autonomous capabilities."[2]

Iran had previously touted the Arash-2 long-range drone as featuring AI-based autonomous navigation, electronic-warfare resistance, and radio-frequency homing. Iranian Army spokesman Brigadier General Mohammad Akraminia claimed the platform was used in an alleged strike on Israel's Ben Gurion Airport on March 21, 2026, which was announced as a precision strike against airport infrastructure and fuel depots.[3] According to sUAS News, the Arash-2's multi-mode guidance package combines a passive radar homing head capable of autonomously detecting, tracking, and hunting enemy radio-frequency emissions with seamless transition to GPS, inertial navigation, or "an optical smart seeker" for the terminal dive. However, neither the AI component nor the Ben Gurion airport strike has been independently confirmed by Israeli or US sources.

AI in Iranian Missiles

Iran's pre-war narrative around its AI-enhanced missile capability was anchored in claims about a specific group of systems — the Abu Mahdi naval cruise missile, the Fath-360 short-range tactical ballistic missile, the Ghadir (Qadir) cruise missile, the Qaem air-to-ground bomb, and the Almas anti-armor missile — most of which were touted publicly by IRGC Navy Commander Rear Admiral Alireza Tangsiri and other military leaders between July 2023 and February 2025. Despite Iran's extensive pre-war emphasis on AI-enabled missile systems, reporting from the March–June 2026 conflict does not confirm the operational use of AI-enhanced missile capabilities in strikes against the US, Israel, or their Gulf partners. Instead, IRGC statements on Operation True Promise 4 highlighted more traditional advantages: the combat debut of the Fattah-2 hypersonic glide vehicle on March 1, massed salvos of Fattah, Emad, and Qadr ballistic missiles, the ability to penetrate layered air defenses such as THAAD, and coordinated missile-drone attacks against US and Israeli targets.[4] [5] IRGC and Khatam Al-Anbiya joint military headquarters statements during wartime invoked "artificial intelligence"

[1] The potential tactical enhancements are based on analysis of Russian drone-related AI capabilities and aspirational technical development from various sources including Center for Strategic and International Studies, The Institute for the Study of War, Forbes, Defense Express, Ukrainian National News, and Ukrainska Pravda.
[2] *https://www[.]presstv[.]ir/Detail/2025/11/12/758687/explainer-why-shahed161-drone-symbolizes-iran-leap-indigenous-defense-tech*
[3] *https://www[.]presstv[.]ir/Detail/2026/03/22/765684/Iran-s-Army-successfully-attacks-Ben-Gurion-airport-using-Arash-2-drones*
[4] *https://www[.]presstv[.]ir/Detail/2026/03/05/764967/United-States-Iran-war-drones-Shahed-IRGC*
[5] *https://wanaen[.]com/55th-wave-of-true-promise-4-operation-targets-tel-aviv-and-u-s-bases-in-the-region/*

only as adversarial targets for its strikes, including specifically threatening to strike Western information technology companies and Gulf-based AI data infrastructure.

Iran's alleged AI-enhanced missile inventory, prominently touted before the war, has not generated wartime claims, wreckage-based attribution, or post-strike assessments from US, Israeli, or Gulf sources. In early December 2025, three months prior to hostilities, the IRGC Navy launched a large-scale exercise that state-run media reported as demonstrating "advanced defensive and offensive capabilities enhanced by artificial intelligence." The exercise, codenamed Shahid Mohammad Nazeri, specifically demonstrated AI's use in air defense systems, including using AI to "identify flying and naval targets in a fraction of the time and hit them with high accuracy" under electronic warfare conditions.[6] However, state-backed media announcements describing successive "waves" of Operation True Promise 4 lacked specific mentions of AI in its missiles — a notable absence given how prominently AI featured in pre-war Iranian missile rhetoric. It is possible that Iran did employ such systems and that either the AI components were not discernible in post-strike forensics or that Iran's use of AI has not been disclosed publicly by either Iran or its adversaries. Furthermore, the most prominent Iranian spokesperson for AI-missile capabilities, IRGC Navy Commander Tangsiri, was killed in an Israeli strike on March 26, eliminating the public-facing voice that had made the bulk of AI-missile claims in the years preceding the war. Even if the Iranian missiles themselves lacked built-in AI capabilities, the IRGC may have benefited from AI-enhanced satellite imagery produced by the Chinese geospatial AI company MizarVision to help identify and tag US and its allies' military infrastructure in the Gulf, according to an Australian Broadcasting Corporation report.

AI in Iranian Naval Operations

Iran has made AI-enabled naval autonomy claims since at least November 2023, when IRGC Navy Commander Tangsiri stated that the IRGC had manufactured unmanned surface vessels (USVs) and unmanned underwater vehicles (UUVs) that use AI to "receive commands, attack a specific target with a desired layout, carry out intelligence operations, and return to the base after carrying out a task."[7] Iran has used USVs during the 2026 war, with the first confirmed Iranian explosive drone boat attack against commercial shipping occurring on March 1, 2026, targeting the Marshall Islands–flagged oil tanker MKD VYOM. According to the CEO of drone technology company Draganfly, such systems can have autonomous capabilities, including "autonomous swarming where they might have 10 boats that can act with a large level of independence, because they're pre-programmed." However, autonomous AI guidance is not a confirmed attribute of the Iranian systems, and the Iranian tactic is consistent with remotely controlled or pre-programmed explosive USVs operating under human supervision, not with autonomous swarming engagement. Neither Iran nor its adversaries have confirmed actual combat use of an Iranian UUV during the war, and AI use in submarine systems remains unproven. Similarly, there is no evidence that the mines Iran laid in the Strait of Hormuz were AI-enabled or autonomous; instead, they are likely conventional naval mines deployed using established IRGC small-craft tactics.

[6] *https://www[.]presstv[.]ir/Detail/2025/12/04/760015/IRGC-navy-launches-major-Persian-Gulf-drill-with-warnings-to-US-ships*
[7] *https://www[.]tasnimnews[.]com/en/news/2023/11/08/2985263/irgc-develops-ai-powered-vessels-submarines*

As such, Iran's naval capabilities during the conflict have been defined by its asymmetric tactics — small boats, mines, explosive remote-controlled USVs, and projectile attacks from IRGC fast attack craft. These naval operations have formed the basis of IRGC naval doctrine in the Strait of Hormuz since the late 1980s, and do not seem to have been updated with the AI-enabled autonomous capabilities Iranian state media had claimed before the war.

Domestic Security

In the limited visibility afforded by Iran's 88-day internet blackout starting January 8, 2026, there is a notable absence of newly documented AI-specific deployments in Iran's domestic repression of the "Dey 1404" protests (referencing the monthlong protests starting late December 2025, during the Persian month of Dey). Even within that constrained information environment, however, two AI-related insights have emerged: Russian-made FindFace facial recognition is a key tool that Iranian authorities very likely employed during the protest crackdown; and established AI surveillance infrastructure, operational in Iran for years to facilitate morality crackdowns after the Woman, Life, Freedom movement, almost certainly enabled the regime's surveillance during that period.

FindFace

An investigation by Forbidden Stories published March 3, 2026, documented that Iran's IRGC- and MOIS-linked surveillance ecosystem has operated the Russian facial recognition system FindFace since August 2019. Forbidden Stories' report, which it claims is based on leaked Russian and Iranian corporate records, indicates that Russian state-affiliated firm NtechLab granted Iranian start-up Rasad Intelligent Technologies (Rasadco) the right to use its software product. Two years later, Kama (Kavoshgaran Marzhaye Danesh Ilia) — a company headed by an IRGC member — took over from Rasadco and distributed the operating licenses throughout Iran, including to other companies that provided software to the IRGC, the Ministry of Defense and Armed Forces Logistics (MODAFL), and MOIS. FindFace allows for "interaction tracking," in which the system creates a "social map" of a targeted individual's relationships. The system saves and integrates data, processes the images, and enables law enforcement to make arrests once resources are available. Although the Forbidden Stories report does not explicitly verify FindFace's operational use during the "Dey 1404" protests, it cites Iranian cybersecurity researcher Nima Fatemi's assessment that "all evidence indicates" the system was operational during the crackdown.

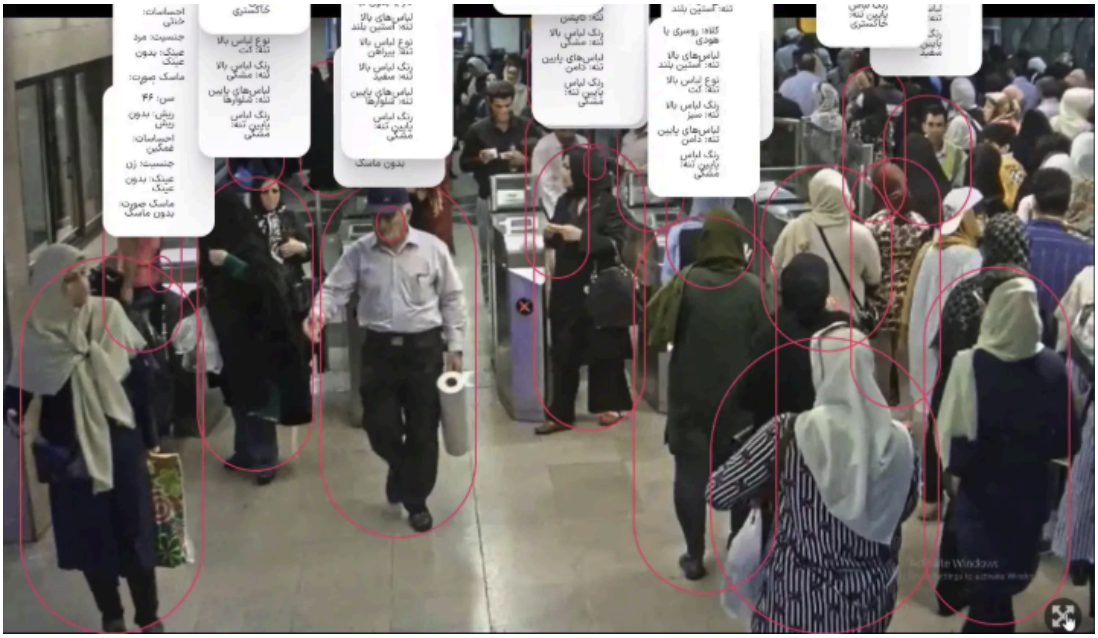

Figure 9: *Screenshot from a video obtained by Forbidden Stories showing the use of FindFace software in a metro station in Tehran, anonymized for privacy protection (Source: Forbidden Stories)*

Surveillance Infrastructure

AI surveillance infrastructure initially put in place to monitor women's hijab compliance during the 2022 Woman, Life, Freedom movement was very likely expanded to monitor and repress the protests that began in December 2025. The UN Independent International Fact-Finding Mission on the Islamic Republic of Iran (FFMI) concluded, in its March 2025 report, that Iran has escalated its use of facial recognition and digital surveillance to suppress dissent, and FFMI's chairperson said, "We are receiving chilling reports on the use by the State of artificial intelligence, including through new mobile apps, to monitor and enforce compliance by women and girls with mandatory hijab rules." Much of this technical architecture is derived from Chinese monitoring tools often obtained through front companies, including deep packet inspection (DPI) technologies for internet traffic monitoring from Chinese telecom companies such as Huawei and ZTE, as well as camera-based visual surveillance technology from Hikvision and Tiandy. A third category of Chinese equipment reportedly enabled "alarming" capabilities through smaller Chinese suppliers, according to researchers at the Outline Foundation and Project Ainita. In May 2025, Iran's and China's Information Technology Ministers pledged to further expand cooperation in information technology, communication infrastructure, and AI.[8] Iran will likely continue to benefit from China's and Russia's AI-enhanced authoritarian capabilities.

Mitigations

- Recorded Future customers can use the platform to detect Iranian threat actor TTPs, defend against Iranian AI malware, understand the risks of AI malware, and identify AI-generated digital content.

[8] *https://www[.]tehrantimes[.]com/news/513061/Iran-China-discuss-ways-to-foster-technological-partnerships?*

- Customers can monitor Recorded Future geopolitical intelligence and cyber threat analysis for updates on Iranian AI enhancements to hybrid warfare tactics impacting their physical and cybersecurity.
- Organizations (including Western and Gulf government agencies, human rights groups, academic and NGO institutions) and industries (IT, defense, energy, logistics, aviation, and maritime) targeted by Iran in 2026 should understand the persistent risks to their digital and physical infrastructure from Iran's asymmetric operations.
- Industries should prioritize awareness and protection against AI-enabled cyber intrusion, social engineering, and IO campaigns.
- Energy and critical infrastructure operators should prepare for both cyber and physical disruption attempts that combine digital attacks with kinetic threats against their operational technology environments, ensuring continuity-of-operations plans are in place to mitigate the impacts.
- Logistics, maritime, and commercial shipping firms with assets in the Middle East should anticipate increasingly sophisticated AI-enabled operations designed to disrupt supply chains and raise operating costs.
- Governments targeted by Iran should prepare to defend against its AI-enhanced hybrid campaigns, including in the cyber, informational, and kinetic warfare realms.

Outlook

Iran's survival amid the unprecedented challenges of 2026 demonstrated that its greatest strategic advantages are derived from asymmetric operations rather than breakthrough AI capabilities. Nevertheless, AI has become an important force multiplier across the cyber and information domains, enabling Iranian state-backed actors to generate cyber effects faster, identify vulnerabilities more effectively, and scale influence campaigns more efficiently. As tensions with its adversaries remain heightened amid fragile diplomacy, Iran's digital capabilities will likely remain active, posing an elevated threat environment for US, Israeli, and Gulf government and commercial networks. Tehran is also likely to continue to leverage AI-enabled propaganda and IOs to shape domestic and international perceptions, portraying any diplomatic accommodation with Washington as a strategic success while discrediting opposition movements and external adversaries.

The collapse of the June 17 memorandum of understanding between the US and Iran very likely reflects that the underlying drivers of instability remain unresolved, increasing the likelihood of ongoing cycles of conflict escalation and diplomacy. Iran will likely prioritize rebuilding the military capabilities that underpin its asymmetric deterrence strategy, including missile and drone inventories, and preserving its ability to threaten maritime traffic and global energy markets through its geographic position near the Strait of Hormuz. Rather than fundamentally altering this approach, AI will likely be increasingly integrated into these capabilities where it provides operational advantages, particularly in targeting support and autonomous systems.

Iran's AI trajectory will also be shaped by deepening cooperation with Russia and China. Russian battlefield experience in Ukraine has accelerated the development of AI-enabled military tactics,

unmanned systems, and operational concepts that could continue to diffuse into Iranian military planning. Additionally, Chinese advances in surveillance technologies, data analytics, and AI-enabled social control provide a model for strengthening Iran's domestic security apparatus. As these partnerships mature, Tehran will likely gain access to capabilities, expertise, and operational lessons that further enhance its hybrid warfare toolkit. The result is not an Iran transformed by AI, but an Iran increasingly capable of integrating AI into an already effective strategy for projecting influence, resisting pressure, and imposing costs on more conventionally powerful adversaries.

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 customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com