Autonomous Weapon Systems in Iran: The New Proxy Warfare Doctrine

May 6, 2026 | SnugLab Research | readme.snuglab.com

Executive Summary

While Iran increasingly integrates autonomous weapon systems (AWS), particularly drones, into its proxy networks to impose asymmetric costs on adversaries, the available evidence suggests these systems do not yet constitute a fundamentally new proxy warfare doctrine centered on machine-level decision-making. Instead, Iran's AWS operations remain constrained by human supervision, reliance on predictive algorithms, and vulnerabilities to supply chain interdiction and command-and-control disruptions. These systems function more as adaptive force multipliers within a human-led, albeit degraded, proxy architecture, rather than fully autonomous strategic anchors.

Key Findings

Iran's "Autonomous" Systems Rely on Human Oversight and Predetermined Algorithms

Iran's claims of utilizing AI for target detection and autonomous operation in its drone and missile programs do not reflect genuine, independent machine-level decision-making [14]. Experts remain skeptical of Iran's autonomy claims, citing the country's history of exaggerating technological achievements [1]. Most military AI applications, including Iran's, function as decision-support systems where humans retain ultimate authority over targeting and engagement [9]. For instance, Iranian swarm technology is designed to operate based on "predetermined information" or ground control, rather than real-time machine reasoning [14]. This limitation is exacerbated by severe wartime infrastructure degradation, including U.S. and Israeli strikes that have caused near-total internet blackouts, reducing connectivity to 1-3% of normal levels [5, 1, 2, 3, 4, 6]. This lack of networked communication forces Iranian systems to rely on isolated predictive algorithms and human-supervised controls, hindering true autonomous battlefield decision-making [5, 14].

US Interdiction Disrupts Near-Term Production, but Adaptive Networks Sustain Long-Term Deployments

Sustained US-led supply chain interdiction severely disrupts Iran's near-term AWS production capacity by severing critical component imports. The United States and its allies are systematically targeting procurement networks across Asia, the Gulf, and Europe for components such as servomotors, carbon fiber, accelerometers, and gyroscopes [8, 10]. These efforts, including AI-assisted financial enforcement and ecosystem-level sanctions, have severely impacted Iran's command structure and immediate ability to conduct coordinated operations [5, 7]. Operation Epic Fury, for example, significantly impacted Iran's ability to develop and deploy autonomous systems [4, 5].

However, Iran has developed structural mechanisms to counter these disruptions. Its military-political system employs an antifragile "mosaic doctrine" designed to adapt and regenerate capacity under pressure, establishing pathways to replace lost nodes [7]. Iranian commanders are also integrating lessons from the Russia-Ukraine conflict to build resilient defense production capabilities, explicitly adopting 3D printing (additive manufacturing) for low-cost drone manufacturing to bypass traditional supply chain vulnerabilities [12]. Consequently, while interdiction collapses immediate, coordinated AWS deployment capacity, these adaptive procurement strategies and additive manufacturing techniques establish a resilient feedback loop that sustains proxy deployments over the long term [7, 12].

Iranian Drone Operations Impose Asymmetric Costs but Fail to Validate Autonomy Claims

The operational record of Iranian drones in Ukraine and against regional proxies demonstrates a tension between economic asymmetry and tactical effectiveness, ultimately failing to validate Tehran's assertion that autonomous systems can reverse the structural degradation of its proxy doctrine. Russia's deployment of Iranian-made Shahed drones in Ukraine has served as a live testing ground, providing real-world feedback and facilitating technical intelligence exchanges [12]. During the 2026 Iran War, Shahed-series one-way attack drones were used to strike Israel, US military bases, and allied nations [5, 8, 13, 15]. These drone swarm attacks are designed to impose "exponential costs" on adversaries, forcing expensive high-end air defenses to intercept cheap aerial threats; Shahed drones are estimated to cost between $20,000 and $50,000

each, while interceptors can cost 20 to 30 times that amount [13, 15, 5].

Despite this cost-imposition strategy, it does not equate to battlefield reliability or strategic success. During Operation Epic Fury, Iran's proxies proved largely ineffective, and Tehran's initial response was one of "damage limitation," reflecting an inability to sustain direct warfare [4]. US and Israeli kinetic and cyber strikes severely disrupted Iran's command structure and internet infrastructure, hampering coordinated drone operations [5]. Experts remain skeptical of Iran's claims of advanced AI-guided and fully autonomous capabilities due to its history of technological exaggeration [1]. The operational record shows that autonomous systems have not compensated for the intelligence penetration, leadership losses, and financial constriction that have dismantled Iran's proxy architecture since October 7, 2023 [4].

US Kill Chain Compression Drives Decentralized Drone Swarms

The US military's AI-driven compression of the targeting kill chain has severely disrupted Iran's centralized command structure and near-term ability to conduct coordinated state-directed operations, yet it has not dismantled Iran's capacity for asymmetric warfare. Instead, it reinforces a tactical pivot toward decentralized, low-cost drone swarms. Systems like the Maven Smart System (MSS) compress the targeting process from days to seconds, enabling rapid strikes that destroyed much of Iran's conventional military infrastructure in under three weeks [1, 11, 2, 5, 6]. These operations severely disrupted Iran's command structure and internet connectivity, hindering coordinated state-directed responses [5].

This US advantage has incentivized Iran to rely on decentralized, low-cost aerial threats. Iran continues to deploy Shahed-series drones to impose "exponential costs" on advanced defenses, leveraging the economic asymmetry where cheap drones require expensive interceptors [13, 15]. Iran's "mosaic doctrine" is designed to be antifragile, expecting to lose individual nodes but having pathways for replacement [7]. Iran is also actively refining its battlefield doctrine by analyzing the Russia-Ukraine war, focusing on resilient defense production, 3D printing for low-cost drone manufacturing, and widespread small-drone/AI integration [12]. While these decentralized swarm tactics impose disproportionate economic costs, analysts note that Iran's proxies were largely ineffective in sustaining direct warfare during Operation Epic Fury [4].

Automation Fails to Enhance Precision; Legitimacy Erodes from Structural Degradation

Iran's increasing reliance on automated decision-support systems has not successfully enhanced operational precision or strategic deterrence within its proxy networks. Tehran's declining political legitimacy and influence projection are primarily driven by the structural degradation of its proxy architecture and severe command-and-control disruptions, rather than collateral damage caused by automation bias. While Iran pursues AWS and AI as force multipliers, developing AI-guided suicide drones and swarm technologies to impose "exponential costs" [14, 15], these ambitions have not translated into battlefield success. During the 2026 conflict, Iran's proxies proved largely ineffective, and its response was initially one of "damage limitation" [4]. US and Israeli kinetic and cyber strikes severely disrupted Iran's command structure and internet infrastructure, crippling the coordination required for both human-led and automated proxy operations [5]. Skepticism persists regarding Iran's technical capabilities due to its "history of shameless exaggeration" concerning autonomous systems [1]. The erosion of Iran's political legitimacy and long-term influence projection stems from the multifaceted degradation of its "mosaic doctrine"-exacerbated by sanctions, military attrition, intelligence penetration, leadership losses, and financial constriction-rather than autonomous decision-making errors within its proxy ranks [4].

Lack of Explicit Human-in-the-Loop Protocols

The provided research does not contain any named Iranian military directives, IRGC operational manuals, or procurement contracts that explicitly define human-in-the-loop oversight protocols for autonomous weapon systems deployed to proxy networks [6, 9]. While the documents confirm Iran's use of drones and artificial intelligence in cyber operations and by its proxy forces, specific internal Iranian policies or named directives regarding human oversight for these autonomous systems are not detailed.

Implications

The findings suggest that while autonomous weapon systems are a significant and evolving component of Iran's proxy warfare, they are primarily used as force multipliers for asymmetric cost imposition rather than as the central pillar of a new, fully autonomous doctrine. The US military's advanced AI integration and kill chain compression have

effectively disrupted Iran's centralized command, pushing Iran towards more decentralized, low-cost drone swarms. This tactical adaptation allows Iran to continue projecting influence and imposing economic costs despite its proxy architecture undergoing structural degradation. However, the operational record indicates that these systems have not reversed the overall ineffectiveness of Iran's proxies in sustained direct warfare, nor have they overcome the fundamental reliance on human oversight and resilient, adaptive supply chains. For stakeholders, this implies a continued need to counter Iran's adaptive procurement and manufacturing capabilities, while recognizing that the strategic impact of its AWS remains limited by human-centric command structures and technological constraints.

Limitations and Caveats

This report's conclusions are provisional, particularly given the "Low confidence" assessment from the framing debate, which noted a lack of direct arguments or evidence presented on the core question. The research relies heavily on external analysis and observations of Iranian capabilities and operational outcomes, rather than direct access to internal Iranian military doctrine or explicit policy documents. Specifically, there is no explicit evidence within the provided sources detailing named Iranian military directives or protocols for human-in-the-loop oversight of autonomous weapon systems. This absence limits the ability to definitively assess the extent of genuine machine-level decision-making versus human supervision within Iran's AWS programs. Furthermore, several key sources ([1], [4], [5], [12]) were cited across multiple findings, indicating a relatively concentrated evidence base.

Sources

[1] How Ai Is Rewriting The Rules Of Modern Warfare - visionofhumanity.org - https://www.visionofhumanity.org/how-ai-is-rewriting-the-rules-of-modern-warfare/

[2] Irans Proxy Strategy And The Extent Of Surrogate Autonomy - alexanderhamiltonsociety.org - https://alexanderhamiltonsociety.org/security-strategy/issue-two/irans-proxy-strategy-and-the-extent-of-surrogate-autonomy/

[3] 8 Vaughan2125 - iiss.org - https://www.iiss.org/globalassets/media-library---content--migration/images/comment/analysis/2017/december/8-vaughan2125.pdf

[4] Degradation Irans Proxy Model - belfercenter.org - https://www.belfercenter.org/research-analysis/degradation-irans-proxy-model

[5] Cyber Strategy Under Fire Iranian Apt And Proxy Retaliation - blog.polyswarm.io - https://blog.polyswarm.io/cyber-strategy-under-fire-iranian-apt-and-proxy-retaliation-risks

[6] Ai Autonomous Weapons Danger Human Judgment 13994708 - firstpost.com - https://www.firstpost.com/opinion/ai-autonomous-weapons-danger-human-judgment-13994708.html

[7] [gov] 3 5 Antifragile War Iranian Mosaic Doctrine Agentic Ai And H - futurium.ec.europa.eu - https://futurium.ec.europa.eu/en/apply-ai-alliance/community-content/3-5-antifragile-war-iranian-mosaic-doctrine-agentic-ai-and-how-prevent-perpetual-war

[8] [gov] Economic Fury Targets Iranian Missile And Uav Procurement Networks - editorials.voa.gov - https://editorials.voa.gov/a/economic-fury-targets-iranian-missile-and-uav-procurement-networks/8141811.html

[9] [edu] Us Military Leans Ai Attack Iran Tech Doesnt Lessen Need Hum - research.gatech.edu - https://research.gatech.edu/us-military-leans-ai-attack-iran-tech-doesnt-lessen-need-human-judgment-war

[10] Disrupting Procurement Networks Supporting Irans Unmanned Ae - iranwatch.org - https://www.iranwatch.org/library/governments/united-states/executive-branch/department-state/disrupting-procurement-networks-supporting-irans-unmanned-aerial-vehicle-uav

[11] [blog] Three Wars In One Ai Adaptation And - scsp222.substack.com - https://scsp222.substack.com/p/three-wars-in-one-ai-adaptation-and

[12] Articleshow - timesofindia.indiatimes.com - https://timesofindia.indiatimes.com/defence/international/how-iran-is-learning-from-ukraine-war-drones-ai-and-a-new-military-playbook/articleshow/130384367.cms

[13] [commentary] Irans Drone Swarm Attacks Unleash Exponential Costs Us Prolo - foxnews.com - https://www.foxnews.com/world/irans-drone-swarm-attacks-unleash-exponential-costs-us-prolonging-war-asymmetric-capability

[14] Irans Bet On Autonomous Weapons - warontherocks.com - https://warontherocks.com/irans-bet-on-autonomous-weapons/

[15] Btr Us Military And Intelligence Agencies Turn Supply Chain - natlawreview.com - https://natlawreview.com/press-releases/btr-us-military-and-intelligence-agencies-turn-supply-chain-mapping-degrade