AI Accelerated U.S. Operations in Iran. Now It's Time to Rethink the Human Role.

by Patricia Brennan **(/experts/patricia-brennan)**

Nov 2, 2026

ABOUT THE AUTHORS



Patricia Brennan (/experts/patricia-brennan)

Lieutenant Colonel Patricia C. Brennan is the 2026-27 Department of the Air Force Fellow at The Washington Institute, where her work focuses on airpower and the implications of contemporary conflict for U.S. defense strategy and military operations. Brennan was previously the commander of the 303d

Brief Analysis

The conflict has demonstrated how AI-enabled warfare can accelerate the "kill chain," but human analysts must still know when to question machine recommendations in order to avoid harmful operational or strategic consequences.

During Operation Epic Fury, U.S. forces reportedly **(https://www.forbes.com/sites/mikebrown/2026/03/30/the-first-ai-war-how-the-iran-conflict-is-reshaping-warfare/)** struck more than 1,000 targets within the first twenty-four hours and more than **(https://www.centcom.mil/Portals/6/Documents/Publications/260401-Fact%20Sheet.pdf)** 13,000 targets within thirty-eight days. According to U.S. Central Command chief Adm. Brad Cooper, the United States achieved **(https://www.war.gov/News/News-Stories/Article/Article/4487365/centcom-commander-says-epic-fury-crippled-iran-enhanced-military-partnerships-i/)** its military objectives in less than forty days by "degrad[ing] Iran's ability to project power outside its borders and threaten the region and...our interests." He also noted **(https://defensescoop.com/2026/03/11/us-military-using-ai-against-iran-operation-epic-fury-adm-cooper/)** that CENTCOM's integration of artificial intelligence had helped compress processes that previously took hours or days into seconds, highlighting the potential operational advantages of AI-enabled systems. These advantages were not limited to faster targeting—they also included the rapid dissemination of critical threat intelligence to U.S. aircraft operating in contested skies. Lt. Gen. Michael Conley, the head of Air Force Special Operations Command, credited **(https://www.militarytimes.com/news/your-military/2026/05/13/ai-tool-has-saved-a-lot-of-aircraft-in-epic-fury-afsoc-chief-says/)** AI with reducing intelligence dissemination to the cockpit from around twenty or thirty minutes to just two or three seconds, making American crews safer from Iranian threats.

For decades, the U.S. military has invested **(https://www.brennancenter.org/our-work/research-reports/militarys-use-ai-explained?)** in technologies aimed at reducing the manpower and time required to identify and geolocate targets, thereby shortening the "kill chain." The Iran war demonstrated **(https://www.cfr.org/event/ai-drones-and-the-war-in-iran?)** the potential operational payoff of these investments, with AI-enabled systems fusing hundreds of intelligence sources to generate targeting recommendations at unprecedented speed and scale. At the center of these capabilities **(https://thehill.com/opinion/technology/5790157-ai-military-revolution-warfare/)** was Palantir's Maven Smart System, which integrated intelligence across various sources and platforms to identify and prioritize targets. Anthropic's Claude provided an additional reasoning layer within Maven, while Anduril's Lattice integrated sensor data to support situational awareness and autonomous operations.

Of course, AI-enabled warfare is not new to the Middle East. Israel has employed **(https://artificialweapons.com/case-studies/israel-ai-targeting-gaza)** Gospel, Lavender, and other AI-assisted targeting systems to fuse intelligence and generate target recommendations for years. More recently, CENTCOM reportedly **(https://agsi.org/analysis/ai-is-reshaping-the-yemen-battlefield/)** used a Maven-like tool to support Saudi target development and intelligence sharing against Houthi forces in Yemen. It also announced **(https://www.centcom.mil/MEDIA/PUBLIC-RELEASES/Article/4557279/centcom-to-launch-1st-bilateral-ai-task-force-with-uae/)** America's first bilateral military AI task force with the United Arab Emirates. These developments show that AI is becoming increasingly integrated into military operations across the region, underscoring the importance of broadly applying the lessons learned from Operation Epic Fury.

Yet one of the most important lessons is that closer examination of AI's role in the targeting process is warranted before these powerful capabilities become more widely integrated across U.S. and partner operations. It remains unclear how accurately AI performed during the height of the war, how effective the strikes were, or the extent to which human operators relied on AI. And regardless of the results in this particular conflict, targeting at machine speed creates the general risk that human decisionmakers will become either a bottleneck or a rubber stamp in the process, with potentially adverse operational and strategic implications in either case.

This tension extends beyond individual targeting decisions, perhaps affecting how Washington prosecutes wars. AI may give U.S. forces the ability to strike thousands of targets in quick succession, but greater targeting capacity does not necessarily equal greater strategic effect. If the availability of targets begins to drive what gets struck, the targeting process could wind up determining strategy rather than serving it. This is particularly consequential in a sustained military campaign, where finite munitions must be prioritized against targets that contribute most directly to achieving U.S. objectives.

The Risks of Overreliance on AI

As CENTCOM expands AI cooperation across the region, the challenge will extend beyond simply determining which technologies should be transferred to which partners and when. Washington must also ensure that U.S. and partner forces are prepared to critically evaluate AI-generated recommendations. This is especially important as AI's processing speed gives analysts less time—and potentially less incentive—to interrogate machine-generated recommendations. Under wartime pressure, the delays caused by additional human validation could lead personnel to rubber-stamp AI recommendations rather than serve as an additional layer of due diligence **(https://www.brennancenter.org/our-work/research-reports/militarys-use-ai-explained?)** .

One way to prevent this is by making sure that analysts do not confuse two different things: machine confidence and target confidence. Traditionally, analysts develop target confidence by examining historical and current intelligence and requesting additional collection to develop an intimate familiarity with the target. Yet AI-generated recommendations change this paradigm: rather than developing confidence in a target, analysts receive an already framed recommendation and are asked to validate it. Developing target confidence and validating machine confidence after the fact are two distinct cognitive tasks, and the danger is mistaking the machine's confidence for sufficient confidence in the target itself.

This distinction matters because AI can process information correctly yet still produce an erroneous recommendation when the underlying data is outdated or has been deliberately manipulated. Consider the U.S. strike on an Iranian girls' school in February, which killed more than 160 people. Reporting **(https://www.theguardian.com/news/2026/mar/26/ai-got-the-blame-for-the-iran-school-bombing-the-truth-is-far-more-worrying?)** suggests that the site remained identified as a military target in a Defense Intelligence Agency database, and that imagery **(https://www.cfr.org/event/ai-drones-and-the-war-in-iran?)** may not have clearly reflected its partial conversion to civilian use. Beyond the loss of life, the strike undermined U.S. strategic messaging and enabled Tehran to claim **(https://www.aljazeera.com/news/2026/7/16/iran-condemns-barbaric-us-attack-near-childrens-cancer-hospital)**

that American forces had committed a war crime. Although the investigation is ongoing and AI's role in the tragedy has not yet been established, the incident illustrates a potential vulnerability: AI-enabled targeting could magnify errors by accelerating the kill chain before analysts identify outdated or contradictory intelligence. The right balance of human scrutiny is therefore critical to establishing reliable target confidence without sacrificing AI's speed advantage.

Appropriately Calibrating Human-Machine Teaming

Achieving this balance requires appropriately calibrated trust in AI-enabled systems. In human automation (https://doi.org/10.1518/hfes.46.1.50.30392) and AI research (https://www.ischool.berkeley.edu/sites/default/files/sproject_attachments/humanai_capstonereport-final.pdf), "calibrated trust" describes the degree to which human operators rely on a system's output based on its assessed capabilities and dependability. In the military context, this means knowing when to rely on AI's targeting recommendations, when to question its outputs, and when to override them. Overreliance could produce targeting errors that undermine broader U.S. policy objectives, while underreliance could result in missed opportunities. In September, for instance, U.S. forces nearly intercepted (https://www.cnn.com/2026/09/18/politics/us-military-ai-false-intelligence-china-ship) a Chinese merchant vessel in the Middle East after an analyst relied on an incorrect AI assessment that the ship's cargo was nuclear-weapons-related. U.S. aircraft were already inbound and personnel were preparing to board the vessel when more experienced analysts discovered the error.

Indeed, the degree of human scrutiny must reflect the nature of the target and the consequences of error. For instance, an excavator in a recently validated Iranian nuclear facility may require less scrutiny than a target that has not been recently vetted and is located amid a civilian populace. The United States has invested heavily in accelerating the kill chain, but recent combat in the Middle East shows why it must invest just as deliberately in ensuring that humans operating within this chain are trained to keep pace—and to keep the proper reins on AI. Even as faster targeting cycles increase the speed and scale of military operations, human analysts must still understand the sources underlying AI recommendations, rapidly recognize contradictory or manipulated information, and know when additional collection or verification is required.

These lessons also extend to a possible conflict with China, a competitor that has the means to challenge U.S. capabilities, sensors, and networks. This could include corrupting AI-enabled targeting at a greater scale and with greater sophistication through false tracks, signal spoofing, decoys, and deepfakes. Anthropic recently identified (https://www.anthropic.com/research/intelligence-targeting-conventional-weapons-capabilities) that AI models perform poorly at identifying signal spoofing—in other words, adversaries do not have to compromise U.S. targeting systems directly if they can persistently manipulate what those systems see.

Given these concerns, the measure of effective AI-enabled targeting should not simply be whether a human remained in the loop. It should be whether that human knew when to trust the machine. An effective human-machine team will preserve judgment without unnecessarily surrendering speed, in part by understanding when the consequences of error warrant slowing the kill chain and when they do not.

Policy Recommendations

In light of the experience (https://www.airandspaceforces.com/former-afcent-commander-reflects-on-lessons-of-epic-fury/) gained during and since Operation Epic Fury, U.S. defense officials should develop a comprehensive AI adoption strategy that strengthens human judgment, builds technical safeguards, continuously assesses AI performance, and incorporates lessons learned from partners, with a focus on the following elements:

Assessing AI performance in the Iran conflict. The Pentagon should commission external reviews of AI performance in combat operations, including the accuracy of AI-generated targeting recommendations and the extent to which humans relied on or challenged these outputs.

Building AI literacy across the military. The Pentagon should incorporate AI literacy into formal training for analysts, repeatedly exposing (https://www.bing.com/ck/a?!&&p=532d1babe114f879267edd24dc7b5e0ef24b913db90ca90f01f017bc79bebc62JmltdHM9MTc5MDEyMTYwMA&ptn=3&ver=2&hsh=4&fclid=0c0723170f7-681c-05e4-3464712b6994&psq=ist+here+a+hyperlink+to+this%3a+Nurkin%2c+T.%2c+%26+Siegel%2c+J.+(2023).+Battlefield+applications+for+human-machine+teaming%3a+Demonstrating+value%2c+experimenting+with+new+capabilities%2c+and+accelerating+adoption.+Atlantic+Council&u=a1aHR0cHM6Ly93d3cuYXRsYW50a them to such technology under realistic conditions. Exercises should incorporate outdated intelligence, adversary deception, degraded sensors, and algorithms of varying reliability, requiring analysts to assess their own performance and gauge whether their level of reliance on AI was appropriate.

Developing machine-on-machine validation models. Future targeting architecture should incorporate independently developed models and sensors to identify contradictions or anomalies in AI-generated recommendations. These models should be tested against human and human-machine performance to determine whether independent machine validation improves error detection. Such validation should augment rather than replace human scrutiny, providing an additional safeguard.

Expanding dialogue with allies and partners. CENTCOM should organize regular Middle East dialogues on lessons learned, building on existing AI-related engagement with Israel (https://www.congress.gov/119/bills/hr8800/BILLS-119hr8800eh.pdf), Saudi Arabia, and the UAE (https://www.commerce.gov/news/press-releases/2025/05/uae/us-framework-advanced-technology-cooperation). The Pentagon should also expand the conversation globally to develop shared approaches to AI-enabled targeting, based on established best practices in human-machine teaming and consistency with the law of armed conflict.

Integrating additional AI guardrails. The Pentagon should incorporate technical safeguards that flag potentially stale or poisoned data, clearly identify machine-generated contributions within finished intelligence products, and require independent validation of target locations and sensor data underlying AI-generated targeting recommendations.

Lt. Col. Patricia Brennan is the 2026-27 Department of the Air Force Fellow at The Washington Institute. Previously, she commanded the 303rd Intelligence Squadron at Osan Air Base in South Korea. The opinions, conclusions, and recommendations in this article are hers alone and do not represent the official positions or policies of the Air Force or any other U.S. government entity. ❖

RECOMMENDED

ARTICLES & TESTIMONY

France's Gulf Moment: Between Momentum and Commitment

October 2026

◆

Souhire Medini

(/policy-analysis/frances-gulf-moment-between-momentum-and-commitment)



ARTICLES & TESTIMONY

The Islamic State's Quiet War on Israel

Oct 29, 2026

◆

Aaron Y. Zelin

(/policy-analysis/islamic-states-quiet-war-israel)



ARTICLES & TESTIMONY

Four Things to Watch in Shipping and Energy If Middle East Conflict Resumes

Oct 30, 2026

◆

Noam Raydan

(/policy-analysis/four-things-watch-shipping-and-energy-if-middle-east-conflict-resumes)

TOPICS

Military & Security (/policy-analysis/military-security)

REGIONS & COUNTRIES

Iran (/policy-analysis/iran)