How AI Is Powering U.S. Strikes on Iran

From the very first day of the war, the American-Israeli strikes on Iran have not relied solely on pilots and traditional battlefield planning. Instead, they have been supported by a dense algorithmic infrastructure that converts images, communications, and vast streams of data into a constantly evolving target bank.

How, then, does raw information an image, a signal, a phone call transform into a classified target and ultimately into an actual strike? And how do the United States and Israel integrate artificial intelligence into targeting, analysis, and battlefield assessment?

First: Algorithmic Surveillance and Satellite Analysis

One of the primary roles of artificial intelligence in the current conflict is processing the immense volume of imagery and geospatial data coming from satellites, drones, and radar systems. Among the most prominent American examples are the following:

1. The “Smart Maven” System

This platform gathers and analyzes enormous quantities of surveillance data from satellites, drones, wireless communications, and the internet. It then fuses this information into a single operational interface that allows U.S. command centers to quickly search for and filter targets, accelerating the decision to strike.

The Maven system collects and analyzes massive amounts of surveillance data.

The system evolved from the original Project Maven developed by Palantir. According to a report by The Washington Post, it has been used in the war against Iran.

2. The Claude System

Developed by Anthropic in cooperation with the U.S. Department of Defense, Claude was designed to accelerate military planning, improve intelligence analysis, and support decision-making related to targeting operations.

The system relies on machine learning to identify targets, prioritize them, and determine the most appropriate strike method. It takes into account previous weapons inventories and past weapon performance against similar targets. It also employs automated reasoning to provide preliminary legal justification for a strike.

The Wall Street Journal revealed that the system was used during the war on Iran as part of what is known as shortening the “kill chain”—the full process from identifying a target to executing the strike.

Beyond Maven and Claude, reports have not confirmed whether Israel used artificial intelligence directly in strikes on Iran. However, several Israeli systems are known to play central roles in modern targeting operations:

1. The “Lavender” System

Developed by Israel’s Unit 8200 intelligence division, this system served as the

backbone of human targeting during the most recent offensive in Gaza.

The algorithm relies on machine learning, training on data from “known individuals” and searching for similar patterns among Gaza’s population to identify potential targets.

2. The “Fire Factory” System

An Israeli system that analyzes operational history data and recommends the amount of ammunition and optimal timing for each strike. In doing so, it connects the stages of target development and capability analysis.

The Fire Factory system focuses on identifying groups of no fewer than five people, and Hebrew-language media reports suggest it has discovered roughly 50 targets annually in recent years.

3. The “Where’s Daddy?” System

This system determines when and where a targeted individual should be killed, representing one of the starkest examples of technological automation in lethal operations.

Traditional military doctrine typically targets fighters while they are engaged in combat activity or present at military facilities. However, Israeli forces faced difficulties locating Hamas fighters within tunnels. According to intelligence sources, the solution was both simple and chilling: wait until they return home.

4. The “Habsora” System

While Lavender and “Where’s Daddy?” focus on individuals, Habsora focuses on infrastructure. It uses artificial intelligence to analyze satellite imagery and structural data to generate building targets at industrial speed.

Habsora expanded the definition of a military target to include what are described as “power targets.” These are not weapons depots or command centers but high-rise residential towers, universities, banks, and public buildings. Such structures are targeted in order to exert massive civilian pressure on the adversary by destroying infrastructure.

Second: Data Integration and Building the Target Bank

The central system in this war is the Smart Maven platform, which gathers data from 179 different sources—from satellites and drones to intelligence reports and converts it into a unified dashboard for military planners.

According to The Washington Post, the system combined with a large language model called Claude generated hundreds of targets, identified their coordinates, and ranked them by priority during planning for strikes on Iran.

Sources familiar with the platform said it is used daily across most U.S. military units and that integrating Claude reduced planning time from weeks to something approaching real time.

The newspaper reported that the system presented targets classified according to strike priority and operational value as determined by planners. It also contributed to post-strike evaluation, suggesting that it oversees the entire targeting cycle from identification to assessment.

According to The Washington Post, the system originally began as a project to detect objects in video footage but later evolved into a comprehensive data-integration platform. Demand for the system grew so rapidly that the Department of Defense expanded Palantir's contract to scale it further.

Even so, the use of Claude remains controversial. The Pentagon has classified its developer, Anthropic, as a "supply chain risk" due to restrictions the company places on military applications. Yet the military continues to rely on the model because it considers it superior to available alternatives.

Despite orders from President Donald Trump to ban Anthropic tools from government agencies within six months, the system continues to operate inside U.S. military platforms.

Third: Analyzing Communications, Language, and Signals

Intercepted communications, daily movement data, and behavioral patterns represent another major domain for artificial intelligence.

A report by the Lawfare website stated that U.S. Cyber Command conducted operations to disrupt Iranian networks during the attack. These operations reportedly relied on infiltrating traffic cameras in Tehran and mobile phone networks to identify the timing of a meeting of Iranian leadership and target it.

Sources speaking to the Financial Times said that a majority of Tehran's traffic cameras had been monitored by Israel and that network intrusions had taken place before the operation began.

Israeli intelligence units use programs like “Where’s My Father?”

The massive volume of communications and imagery cannot be analyzed by humans alone. Here, automated analytics platforms use machine-learning techniques to extract patterns such as Revolutionary Guard gathering locations or movement habits and construct target profiles.

No confirmed information has emerged regarding the exact system used in this field during the current war. However, previous experiences in Gaza suggest Israeli intelligence units rely on software such as “Where’s Daddy?” to analyze lifestyle patterns and determine the moment most suitable for a strike.

There is also a linguistic challenge. Operations against Iran require understanding communications in Persian and Arabic. Technical reports therefore point to the use of language models capable of translating and classifying intercepted communications and integrating them into operational dashboards.

Analysts believe that AI-based translation tools within the U.S. Department of Defense particularly models designed for non-Latin languages may have enabled rapid translation of intercepted orders and messages.

Officials within U.S. Central Command have acknowledged the use of artificial intelligence for what they describe as “data triage.”

Fourth: Target Sorting and Priority Ranking

Once the data is collected, the next step is determining which targets should be

struck first. This is where Maven and Claude perform their most critical role.

The Washington Post reported that the system assigns each target a score based on its importance and proposes sequences for strikes, while also predicting possible responses through scenario simulations.

The platform reportedly prioritized different categories of targets and offered recommendations that planners adopted during the preparation phase.

This ability to rank targets and simulate scenarios has led observers to describe the current conflict as approaching a model of “algorithmic killing,” in which military commanders increasingly rely on algorithms to determine the chronological order of strikes.

Fifth: Measuring Strike Impact and Destruction

U.S. officials say artificial intelligence is not limited to target selection but also plays a role in assessing damage after strikes.

According to The Washington Post, the smart system analyzes the results of attacks and helps determine whether the operation achieved its objectives. This assessment requires combining new satellite imagery with other intelligence data.

Even so, the process remains sensitive. Commercial companies such as Planet Labs have reportedly declined to publish real-time satellite images of the Gulf region after the strikes, fearing that adversaries might use them for damage assessment.

This limitation highlights how information warfare intersects with commercial and political interests. It also demonstrates that reliance on artificial intelligence does not eliminate the need for human and technical intelligence sources.

In sum, the war on Iran does not appear—at least so far—to be a conflict in which artificial intelligence merely plays a supporting role. Rather, algorithms seem to be penetrating the very core of the kill chain: from capturing an image and intercepting a signal, to identifying a name, prioritizing a strike, and measuring the destruction left by the bombs.

What this war reveals is that Washington and Israel are not only using artificial intelligence to accelerate military decision-making, but also to shrink the distance between information and killing to an unprecedented degree.