Mean Machines

The use of AI in war is not entirely new. What is new is how it is setting the pace of human decision-making, says **Mathures Paul**

OLD WAR: A still from the film 300, a creative take on the Battle of Thermopylae between the Persians and the Greeks in 480 BCE. Humans still **wielded their weapons instead of the other way around. Weaponry included falcatas, swords, spears, battle daggers and impressive shields**

Within a week of the start of military strikes against Iran towards the tail end of February, the US managed to hit more than 2,000 targets, including 1,000 within the first 24 hours. Admiral Brad Cooper, the head of Central Command (Centcom), said the first 24 hours of the operation were nearly "double the scale" of the first day of "shock-and-awe" strikes on Iraq in 2003.

AI has played a critical role in the initial screening of incoming data. Captain Timothy Hawkins, a Centcom spokesperson, told *Bloomberg*, "Centcom uses a variety of AI tools — and that is exactly what they are, tools — to assist human experts in a rigorous process aligned with US policy, military doctrine as well as the law."

"When decisions are made in seconds, 'human control' cannot realistically mean a person is making each decision in real time. In those environments, compressed timelines for decision-making force a shift toward autonomous or AI-assisted systems that can operate in sub-second timeframes," a CloudSEK spokesperson told **The Telegraph**.

CloudSEK is a Bengaluru-based predictive cyber-threat intelligence platform. "In practice, most 'human control' exists before deployment, in the form of clear, unambiguous objectives and rules of engagement, along with robust operational guardrails. Once systems are active, human role becomes supervisory at best and often reactive, stepping in after outcomes. This turns control into collateral or damage management rather than direct decision-making," the spokesperson added.

The use of AI on the battlefield is just getting started. There have been reports of Claude, the AI model developed by Anthropic, being used by the US military during its operation to capture Nicolás Maduro from Venezuela. Israel also used AI in Gaza. The war with Iran is adding colour to the urgency of controlling the future of AI as a tool of war, but the story began unfolding much earlier than most of us are aware.

In 2017, when OpenAI was just a bumblebee in a Silicon Valley corporate room and Anthropic was still years away, a unique project was taking wings. The idea behind Project Maven was to use computer vision to trawl through thousands of hours of drone footage taken across Asia, especially West Asia.

It was about bringing intelligence directly into combat operations and testing emerging technology in real wars. The idea far exceeded the use of AI for surveillance.

"You don't buy AI like you buy ammunition," wrote Colonel Drew Cukor in the Department of Defense (now Department of War) news service. "There's a deliberate workflow process." Cukor is one of the key people behind Project Maven, which originally took off under Robert O. Work, the US deputy secretary of defence for both the Obama and Trump administrations from 2014 to 2017.

It might be of interest to note that Cukor has been described as the "founding father of AI targeting".

With large language models integrated into the Maven platform, the number of targets that could be hit per day has increased.

Not everyone in Big Tech — which constitutes Microsoft, Apple, Alphabet (Google), Amazon and Meta — is thrilled. In 2018, thousands of Google employees signed a letter protesting the company's involvement in Maven.

Like ripples in a pond, such protests did not deter organisations like the National Security Commission on Artificial Intelligence from urging the US to develop, field and adopt AI weapons of war. The budget for Project Maven continued to swell. And justification for pushing AI for war came in the form of the spectre of the US losing a major global war.

Right now though the question is how something like Claude, which can also help draft marketing emails, is mixed into the picture of bombings in Iran.

AI & You

A recent *Wall Street Journal* report said it was used for intelligence assessments, target identification and for simulating battle scenarios during the strikes. The report appeared around the same time that Trump ordered federal agencies to stop using Claude after a dispute with its maker.

Secrecy remains central to these operations, and how Claude was used in something like Operation Epic Fury is unclear. In July 2025, Anthropic signed a deal with the Pentagon to integrate Claude into military operations.

Then came the standoff between Anthropic and the US government this year — it revolves around the company's refusal to allow the defence department to use its Claude AI model for fully autonomous lethal weapons or domestic mass surveillance.

The software-driven approach to warfare has deepened since the early days of Maven, forcing the Pentagon to look to the private sector for help. China too is moving fast. Last year, the Chinese air force released a video of its GJ-11 stealth attack drone flying alongside and linked to the J-20 fighter jet.

"Technology has always shaped the nature of warfare but never at this pace. From chemical weapons to nuclear arsenals to commercial spyware, the pattern has been — deployment first, understanding next and then regulation. With AI, that lag is no longer measured in decades. We are already in an agentic phase wherein systems can plan, execute and adapt autonomously, while much of the policy world is still grappling with earlier, simpler models," the CloudSEK spokesperson said.

He said the direction that effective global regulation of AI in warfare must take is clear. First, there must be strict controls on who can develop and deploy frontier AI for autonomous lethal applications. Second, human accountability must remain central for high-consequence decisions, especially for targeting, escalation and anything involving loss of life. Third, there must be meaningful transparency around system capabilities, limitations and deployment contexts. Fourth, there needs to be attribution and deterrence mechanisms that can handle AI-enabled operations at scale, closing the accountability gap that deniability currently exploits.

The future we feared in Hollywood movies is already here.