AI Enters the Intelligence War: America’s Race to Keep Up

Infosources™

July 30, 2025

When China unveiled a powerful large language model (LLM) on the very day of Donald Trump's presidential inauguration, it sent a shockwave through Washington's national security circles. American officials, long confident in their technological edge, were suddenly confronted with the possibility that their rivals—particularly Beijing—were outpacing them in the race to integrate artificial intelligence into military and intelligence operations.

Since then, the global competition to weaponize AI for strategic advantage has intensified. From top-secret deployments inside the U.S. intelligence community to rapid experimentation by military contractors and tech giants, AI is reshaping how national security is conceived, planned, and executed. Across the Atlantic, European agencies are scrambling to stay relevant, while nations like Israel push forward in live combat environments. Yet behind the headlines, adoption remains uneven, capabilities uncertain, and the risks poorly understood.

When China's DeepSeek dropped a powerful large language model (LLM) on the very day of Donald Trump's inauguration, it didn't just make headlines — it rattled the U.S. intelligence establishment. Trump called it a wake-up call. Behind the scenes, senior intelligence figures admitted they were caught off guard.

Since then, the U.S. national security machine — from the Pentagon to the Department of Energy — has been scrambling to keep pace with a rapidly shifting landscape. The Biden administration, recognizing the urgency, has pushed its agencies to work more aggressively with the country's most advanced AI labs: Anthropic, Google DeepMind, OpenAI — and, more recently, Elon Musk's xAI. In July, the Pentagon committed hundreds of millions of dollars to these companies to accelerate research into a new kind of AI: agentic models. These are tools that not only respond to questions but can act on instructions, break down complex tasks, and even command other devices.

Within the intelligence community (IC), AI isn't an experiment anymore — it's active and growing. Microsoft has 26 of its cloud services cleared for classified use. Anthropic launched Claude Gov, a special model fine-tuned for national security agencies. These aren't just chatbot wrappers. They're AI systems embedded into the workflow of spies, analysts, and defense planners. They're trained to recognize sensitive information, understand obscure languages and dialects, and operate in highly secure, isolated networks. The IC isn't just plugging into GPTs — it's reshaping them from the inside out.

Info

LLMs *do not "understand" information in the human sense. Instead, they use statistical patterns from vast datasets to generate plausible-sounding text. When fine-tuned or integrated with government data (e.g., intelligence, intercepted communications, classified files), LLMs can assist analysts in:*

- *Summarizing large amounts of intelligence*
- *Extracting signals from noisy data*
- *Predicting possible developments based on patterns • Generating tailored reports for specific geographies (e.g., the Middle East)*

Info

***Claude Gov** is a **specialized, government-use version** of the Claude LLM by Anthropic, designed to be integrated in **sensitive national security and intelligence environments**.*
***Claude public**: Rejects classified or sensitive docs due to default safety policies.*
***Claude Gov**: **Customized** to **process classified documents**, allowing it to assist U.S. intelligence agencies with tasks like:*

-Parsing vast classified archives

-Extracting relevant intelligence

-Summarizing intercepted comms

Europe is moving, too. In the UK, intelligence officers have top-secret access to generative AI tools. France's AMIAD works with Mistral — the continent's lone AI heavyweight — to build models tailored for intelligence use. Mistral's Saba model is particularly skilled with Middle Eastern and South Asian languages. And in Israel, GPT-4 saw a 20-fold spike in military use after the war in Gaza began.

Info

***Saba** is the codename for an **internal LLM developed by Mistral**, a French AI company and a European competitor to OpenAI. The **Saba model** is:*
*-**Highly performant**, focusing on transparency and open weights -Designed to be **competitive with top-tier U.S. models** -Of interest to **European intelligence** due to its **sovereign, non-U.S.-controlled development***

*Mistral aims to give European actors — including military and intelligence agencies — access to **advanced LLMs without relying on U.S. cloud providers or regulatory oversight**.*

Still, it's not all smooth. Despite the contracts, the headlines, and the political urgency, AI adoption across national security remains sluggish. OpenAI's Katrina Mulligan, who now leads public-sector partnerships, says progress isn't where it should be. Some agencies insist on building their own "wrappers" around public AI models, but the result is often a watered-down experience that lags behind commercial versions. The NSA, long experienced with AI in voice recognition, stands out as a rare center of excellence — but many others lag behind.

Info

How Are LLMs Useful for Intelligence Services — Especially in the Middle East?

LLMs can be trained or adapted to:

*-**Ingest Arabic, Farsi, Hebrew-language content**, including obscure dialects*

*-**Summarize massive surveillance data** (SIGINT, social media, regional news)*

*-**Monitor narrative shifts in online propaganda** (e.g., Iran's influence ops)*

*-**Extract geopolitical insights** from structured and unstructured data*

*-**Answer analysts' questions** interactively like a chatbot, reducing the cognitive load*

What's more, the real challenge isn't just in adopting AI tools — it's in rethinking how intelligence work is done. The mission itself has to be redesigned, argues Tarun Chhabra, a former senior White House official now at Anthropic. Using an LLM as a chatbot is just the beginning. The real transformation begins when the technology rewires how decisions are made, how risks are assessed, how intelligence is collected, analyzed, and acted on.

Yet there's skepticism, particularly among researchers and engineers embedded in institutions like GCHQ and the Alan Turing Institute. They argue that the technology isn't yet reliable enough for the kind of high stakes work intelligence agencies demand. What these institutions need, says AI researcher Richard Carter, is not flashy autonomy but tools that offer consistency, reliability, and transparency. Instead, many labs are racing to develop advanced agentic models — systems that act with initiative, reason recursively, and adapt dynamically to complex environments. These are powerful, but they're also unpredictable. OpenAI's new agentic system "ChatGPT agent" hallucinates more than earlier models, according to internal benchmarks.

The UK, for its part, is mitigating this with techniques like "retrieval augmented generation," where a retrieval system curates trustworthy documents and feeds them into the model — but this is still a workaround, not a foundation. Carter warns that the current LLM architecture isn't built for real-world reasoning. Intelligence agencies, he suggests, should push for a new generation of models designed around causality, logic, and decision-making — not just pattern matching.

Meanwhile, there's China. And that's the wildcard. No one really knows how far Beijing has advanced. DeepSeek's capabilities remain opaque, and Chinese models aren't subject to the same safety constraints and ethical rails as those developed in the West. That could give them an edge — more dangerous, more powerful, more flexible.

Philip Reiner of the Institute for Security and Technology points to a worrying blind spot: the U.S. has done a poor job tracking China's military AI evolution. Penetration of Chinese tech platforms is low, and the intelligence picture is hazy. And so, under pressure, the Trump administration recently ordered regular assessments of how fast American agencies are integrating AI — not just in absolute terms, but relative to rivals like China.

It’s not the speed of innovation that keeps some in the AI labs awake at night. It’s the speed of *adoption*. Katrina Mulligan puts it plainly: America might win the race to AGI — artificial general intelligence — and still lose the race to make it useful.

source: www.economist.com