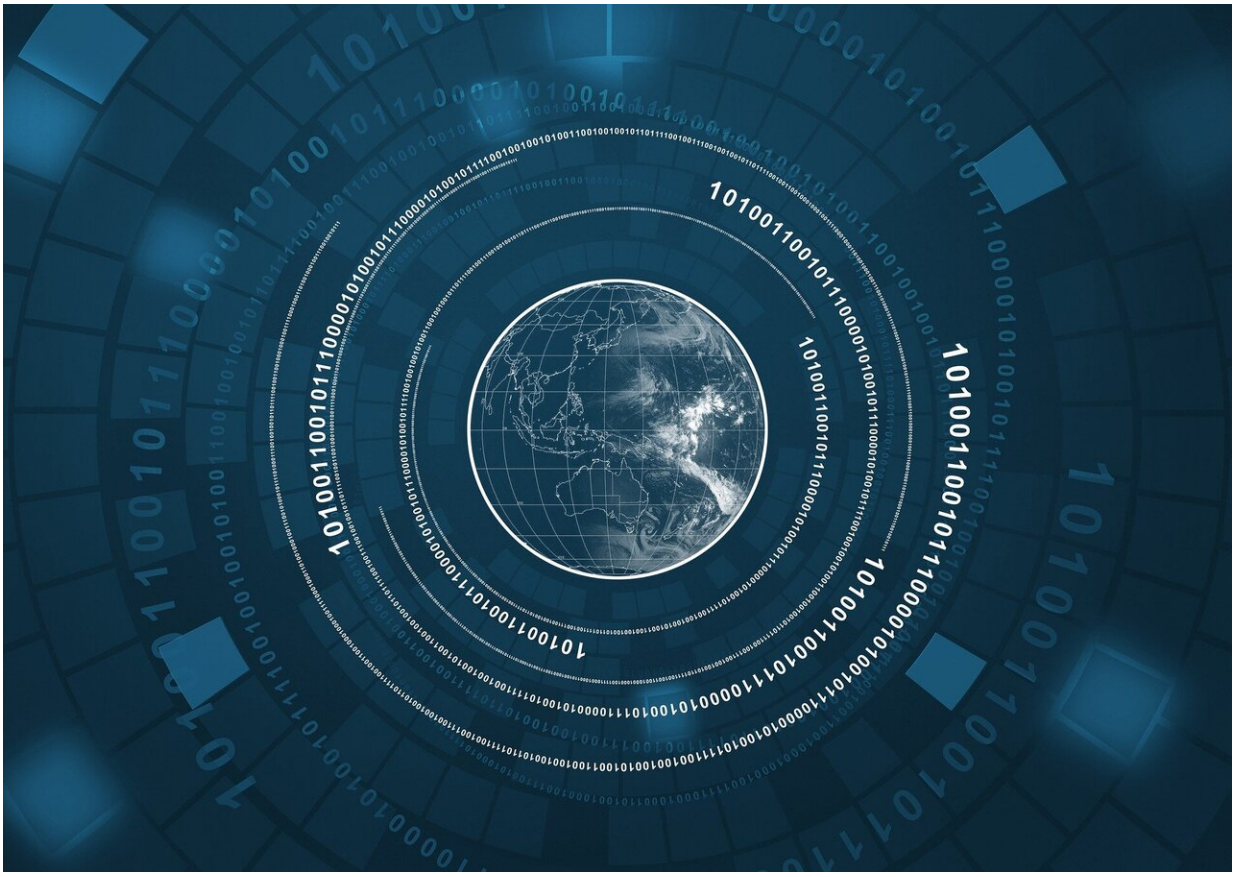
Takeaways: How intelligence agencies' are cautiously embracing generative AI

May 23 2024, by Frank Bajak



Credit: CC0 Public Domain

U.S. intelligence agencies are scrambling to embrace the AI revolution, convinced they'll otherwise be smothered in data as sensor-generated

surveillance tech further blankets the planet. They also need to keep pace with competitors, who are already using AI to seed social media platforms with deepfakes.

But the tech is young and brittle, and officials are acutely aware that generative AI is anything but tailor-made for a trade steeped in danger and deception.

Years before OpenAI's ChatGPT set off the current generative AI marketing frenzy, U.S. intelligence and defense officials were experimenting with the technology. One contractor, Rhombus Power, used it to uncover fentanyl trafficking in China in 2019 at rates far exceeding human-only analysis. Rhombus would later predict Russia's full-scale invasion of Ukraine four months in advance with 80% certainty.

EMBRACING AI WON'T BE SIMPLE

CIA director William Burns recently wrote in Foreign Affairs that U.S. intelligence requires "sophisticated artificial intelligence models that can digest mammoth amounts of open-source and clandestinely acquired information."

But the agency's inaugural chief technology officer, Nand Mulchandani, cautions that because generative AI models "hallucinate" they are best treated as a "crazy, drunk friend"—capable of incredible insight but also bias-prone fibbers.

There are also security and privacy issues. Adversaries could steal and poison them. They may contain sensitive personal data agents aren't authorized to see.

Gen AI is mostly good as a virtual assistant, says Mulchandani, looking

for "the needle in the needle stack." What it won't ever do, officials insist, is replace human analysts.

AN OPEN-SOURCE AI NAMED 'OSIRIS'

While officials won't say whether they are using generative AI for anything big on classified networks, thousands of analysts across the 18 U.S. intelligence agencies now use a CIA-developed generative AI called Osiris. It ingests unclassified and publicly or commercially available data—what's known as open-source—and writes annotated summaries. It includes a chatbot so analysts can ask follow-up questions.

Osiris uses multiple commercial AI models. Mulchandani said the agency is not committing to any single model or tech vendor. "It's still early days," he said.

Experts believe predictive analysis, war-gaming and scenario brainstorming will be among generative AI's most important uses for intel workers.

'REGULAR AI' ALREADY IN USE

Even before generative AI, intel agencies were using machine learning and algorithms. One use case: Alerting analysts during off hours to potentially important developments. An analyst could instruct an AI to ring their phone no matter the hour. It couldn't describe what happened—that would be classified—but could say "you need to come in and look at this."

AI bigshots vying for U.S. intelligence agency business include Microsoft, which announced on May 7 that it was offering OpenAI's GPT-4 for top-secret networks, though the product is not yet accredited

on classified networks.

A competitor, Primer AI, lists two intelligence agencies among its customers, documents posted online for recent military AI workshops show. One Primer product is designed to "detect emerging signals of breaking events" using AI-powered searches of more than 60,000 news and social media sources in 100 languages including Twitter, Telegram, Reddit and Discord.

Like Rhombus Power's product, it helps analysts identify key people, organizations and locations and also uses computer vision. At a demo just days after the Oct. 7 Hamas attack on Israel, Primer executives described how their technology separates fact from fiction in the flood of online information from the Middle East.

CHALLENGES AHEAD AS AI SPREADS

The most important near-term AI challenges for U.S. intelligence officials are apt to be counteracting how adversaries use it: To pierce U.S. defenses, spread disinformation and attempt to undermine Washington's ability to read their intent and capabilities.

The White House is also concerned that generative AI models adopted by U.S. agencies could be infiltrated and poisoned.

Another worry: Ensuring the privacy of people whose personal data may be embedded in an AI model. Authorities say it is not currently possible to guarantee that's all removed from an AI model.

That's one reason the intelligence community is not in "move-fast-and-break-things" mode on generative AI, says John Beieler, the top AI official at the Office of the Director of National Intelligence.

Model integrity and security are a concern if government agencies end up using AIs to explore bio- and cyberweapons tech.

DIFFERENT AGENCIES, DIFFERENT AI MISSIONS

How AI gets adopted will vary widely by intelligence agency according to mission. The National Security Agency mostly intercepts communications. The National Geospatial-Intelligence Agency (NGA) is charged with seeing and understanding every inch of the planet.

Supercharging those missions with Gen AI is a priority—and much less complicated than, say, how the FBI might use the technology given its legal limitations on domestic surveillance.

The NGA issued in December a request for proposals for a completely new type of AI model that would use imagery it collects—from satellites, from ground-level sensors—to harvest precise geospatial intel with simple voice or text prompts. Gen AI applications also make a lot of sense for cyberconflict.

MATCHING WITS WITH RIVALS

Generative AI won't easily match wits with rival masters of deception.

Analysts work with "incomplete, ambiguous, often contradictory snippets of partial, unreliable information," notes Zachery Tyson Brown, a former defense intelligence officer. He believes intel agencies will invite disaster if they embrace generative AI too enthusiastically, swiftly or completely. The models don't reason. They merely predict. And their designers can't entirely explain how they work.

Linda Weissgold, a former CIA deputy director of analysis, doesn't see AI replacing human analysts any time soon.

Quick decisions are often required based on incomplete data. Intelligence "customers"—the most important being the president of the United States—want human insight and experience central to the decision options they're offered, she says.

"I don't think it will ever be acceptable to some president for the intelligence community to come in and say, 'I don't know, the black box just told me so.'"