The Role of Artificial Intelligence in the U.S. Intelligence Community: Current Uses and Future Developments

Jennifer Ewbank

As in many aspects of life and business, artificial intelligence (AI) is transforming the landscape of global intelligence operations. Indeed, the advent of sophisticated AI capabilities is fueling a revolution in intelligence. For the U.S. Intelligence Community (USIC) generally, and the Central Intelligence Agency (CIA) specifically, AI offers unprecedented opportunities to enhance insights and decision-making in intelligence operations and analysis, while streamlining backend business operations for a large, complex, and globally dispersed organization. The integration of AI into the intelligence mission aims to manage the vast amounts of data generated by modern, ubiquitous sensor technologies and assist in the extraction of insights from those data.

The primary mission of the USIC is to provide a decision advantage for the president and U.S. policymakers through the collection and analysis of intelligence. Counterintelligence is also a critical mission, and the CIA adds to these responsibilities covert action, which is conducted at the president's direction. Today, AI plays a growing role in all these missions as a partner to intelligence officers, extracting insights from vast volumes of data and enhancing both the efficiency and effectiveness of intelligence activities. Tremendous progress has been made in recent years, and AI is already changing the intelligence business in profound ways.

AI is instrumental in managing the exponential increase in data generated by ubiquitous sensing technologies and facilitating the integration of these data across various collection "INTs," including human intelligence (HUMINT), signals intelligence (SIGINT), and geospatial intelligence (GEOINT), among others. For instance, the CIA leverages AI for content triage, translation, and transcription to help analysts quickly process vast amounts of information. This is most vividly demonstrated through the OSIRIS platform developed by the CIA's Open Source Enterprise and shared broadly within the USIC.

The CIA's OSIRIS platform showcases the powerful integration of AI in open-source intelligence (OSINT), a mission that, until a few years ago, relied primarily on human expertise and labor. OSIRIS now uses a large language model to synthesize and present vast volumes of OSINT, itself the result of AI-powered workflows, providing summaries and facilitating user engagement through a chatbot. This system builds on decades of human expertise and curated data, guided by subject matter experts and processed at machine speed to deliver actionable insights. It's important to emphasize that OSIRIS does not produce analytic products; rather, it helps the specialist user make sense of massive volumes of OSINT. The chatbot can be used to sharpen thinking, question assumptions, or explore alternative scenarios— all useful functions for the intelligence professional.

Despite recent and impressive advancements in AI, HUMINT remains vital for unlocking powerful insights and delivering a decision advantage for U.S. policymakers. Even with the rapid digitalization of economies around the world, there will always be secrets held only in the minds of dictators, despots, and terrorists—a reality that will only be strengthened as threats across the cyber landscape grow in volume and complexity. Yet, AI still plays an important role in classic espionage—the cloak-and-dagger world of clandestine collection of sensitive intelligence from human sources. AI and machine learning (ML) can enhance HUMINT success by identifying potential intelligence sources (targeting, in intelligence parlance) or constructing digital patterns of life for prospective recruitment targets. Through its interpretation of massive volumes of data, AI can also be a valuable tool in evaluating the digital threat landscape through which intelligence personnel must quietly move and operate around the globe. This partnership between intelligence professionals and AI, between humans and machines, is becoming increasingly critical for success in the digital age.

Beyond HUMINT and analytic missions, AI also enhances business operations within the USIC by automating back-office functions, thereby freeing up human talent for higher-order cognitive tasks. In cybersecurity, AI can

enable rapid responses to unauthorized attempts to penetrate sensitive IT systems, raising defenses at machine speed before bringing in human experts to intervene.

The future of intelligence is inextricably linked to AI, ML, and automation. In an era of exponentially growing volumes of data, the CIA and the broader USIC must achieve an advanced level of AI maturity, or risk obsolescence and irrelevance—potentially on a short timeline. The USIC envisions AI dramatically collapsing timelines from data collection to exploitation. To achieve this, AI and computational power must move to the edge to keep pace with the mission. Given the complexity of the intelligence mission, future AI developments will focus on multimodal models that integrate disparate forms of data collection, such as GEOINT, SIGINT, and HUMINT. These models will reveal new insights hidden in heterogeneous data, enhancing the operational and analytical capabilities of intelligence officers.

Across all efforts to develop and deploy AI capabilities in the USIC, AI ethics, safety, and compliance standards are key areas of focus. Primary goals of these efforts are to reflect respect for human rights, ensure transparency and accountability in AI methods and uses, avoid bias in AI systems, promote public-private partnerships to develop best practices, and strengthen both oversight and training for stakeholders. In brief, the community seeks to reflect our values as a nation as they develop and deploy this new and transformative technology.

Our adversaries, however, are also participants in this race to develop dramatic new AI capabilities, often unbound by legal and ethical frameworks rooted in human rights and data privacy, and so the USIC must now focus on counter-AI measures. This includes studying and assessing adversarial AI capabilities, protecting U.S. AI systems from compromise, and countering adversarial use of AI in misinformation, disinformation, and cyber-attacks, among other priorities.

In terms of nations working at cross-purposes to America's vision of a free, open, and secure cyber landscape, the People's Republic of China's (PRC's) integration of AI into its intelligence and cyber operations already poses significant challenges to global security and democratic systems. The government in Beijing has prioritized AI development, aiming to become the world leader in AI by 2030.

China uses AI to harvest vast amounts of personal data from Americans and other targets, enhancing the efficiency and scale of their own espionage efforts, according to FBI reports. AI also bolsters Chinese hacking operations by processing enormous amounts of data and integrating it across different source streams to create a comprehensive intelligence picture.

Chinese state-sponsored actors also leverage AI to create and distribute disinformation and propaganda. AI-generated deepfakes, manipulated images, and news are used to influence public opinion and sow discord in the U.S. and other countries. AI tools also enhance social media manipulation, exploiting existing societal divisions on issues like climate change, immigration, and U.S. foreign policy.

Russia, similarly, places significant emphasis on using AI in information and cyber operations. The Russian military is developing AI to manage and analyze data from multiple domains, including air, sea, ground, space, and cyber. This multi-domain intelligence approach is enhancing Moscow's ability to gather and process intelligence more effectively. Drones and robotic systems powered by AI are also being used for intelligence gathering, adding a new dimension to Russia's military operations.

Moscow still faces many technological and other hurdles in its development of new AI capabilities, including sanctions. Nevertheless, Russia is actively working to overcome these obstacles through domestic research initiatives, collaboration with their small pool of allies, and investment in AI education.

With a long history of aggressive disinformation campaigns, Russia is now utilizing AI to generate and disseminate disinformation, thereby expanding the speed and scale of influence operations. This includes

creating fake social media content, translating and editing articles, and composing headlines to sway public opinion and influence political outcomes. AI also enhances social engineering tactics, making it easier to craft convincing phishing emails and other deceptive content.

While both nations have ambitious goals for AI in intelligence operations, China clearly represents the most significant challenge to the United States and its democratic allies around the world. AI is a key pillar of China's strategy to achieve global economic dominance and ultimately supplant the U.S. as the world's leading superpower.

China's ambitious AI strategy also strives for the development of artificial general intelligence (AGI), with the potential to blur distinctions between human and machine cognition, potentially leading to even greater levels of societal control by the Chinese Communist Party. In this context, achieving AGI first is a national security imperative for the United States. The race for AGI is not just about technological supremacy or economic advantage; it's about national security and global freedom. Achieving AGI first would provide the U.S. with a significant strategic advantage, ensuring that AI development aligns with democratic values and human rights. Reaching this goal will require strengthening our innovation ecosystem, expanding partnerships between government, industry, and academia, and working closely with like-minded allies, all with the purpose of promoting a positive vision of technology that serves society rather than controls it.

Jennifer Ewbank is a senior national security executive with deep global expertise, who served as Deputy Director of the Central Intelligence Agency for Digital Innovation from 2019 to early 2024. In that role, she led transformation of one of the world's most sophisticated and secure digital technology ecosystems. Ms. Ewbank's blend of technological insight, operational expertise, risk management, global engagements, and support for public-private partnerships is unique in the American national security community and provides a valuable perspective on global security challenges in the digital era. Ms. Ewbank's prior roles at CIA included four tours as Chief of Station, as well as Chief of the former National Resources Division, where she built partnerships with U.S. law enforcement and American citizens and institutions, public and private, to advance the U.S. national security mission. Today, Ms. Ewbank applies her expertise as a board member to strengthen America's economic competitiveness and as a strategic advisor through Andaman Strategic Advisors, of which she is the founder. Ms. Ewbank also continues to share her experience through public speaking engagements for industry and government alike.