U.S. Privacy and Civil Liberties Oversight Board Meeting

11 July 2024

Opening Statement

By

William Usher

Senior Director for Intelligence

Special Competitive Studies Project

Good morning distinguished members of the Board and to those listening in. My name is William Usher and I am the Senior Director for Intelligence at the Special Competitive Studies Project. Our mission at SCSP is to make recommendations that strengthen America's long-term competitiveness in AI and other technologies as they reshape geopolitics and society. Prior to joining SCSP last year, I spent 32 years at the Central Intelligence Agency as an all-source analyst and senior manager. I am honored to speak with you today about the role that artificial intelligence can play in support of U.S. national security, specifically the Intelligence Community's mission.

Today, we find ourselves at a critical juncture in history, where the convergence of geopolitical shifts and technological advancements present both unprecedented challenges and opportunities for our nation's security and global standing. Among these advancements, Artificial intelligence stands out as a transformative force that will profoundly impact national security and global competition. President Biden's Executive Order last October mandated that the U.S. Government departments and agencies take care when developing and deploying AI systems, but it also called on America to take a leading role in developing and deploying this powerful new technology.

- Being a leader in technology innovation is important today, but will be vital to our nation's future economic vibrancy and to the continued resiliency of our democratic way of life.
- For as we debate the future of AI, foreign competitors — principally the Peoples' Republic of China — are laser focused on taking advantage of AI for economic advantage and in some cases to challenge U.S. leadership and the rules-based global order. Beijing has openly declared its aspiration to become a leading S&T power that is able to set the pace for future scientific advancements and dictate global norms.

The Promise of AI for Intelligence

Perhaps the first arena where the power of AI will be most acutely felt is in the world of intelligence. Indeed, our Intelligence Community has long eyed AI's potential and they have been researching the potential uses of early forms of AI — machine learning, deep learning, and natural language processing — for years and have already launched limited uses of generative AI tools.

- I predict these tools will eventually revolutionize how intelligence agencies collect and analyze information, and — if handled correctly — AI tools have the potential to greatly expand the scale and the efficiency with which our intelligence services can derive national security-relevant insights from the growing body of digital information produced around the globe.
- U.S. intelligence services, for example, will be able to leverage AI systems' pattern recognition capabilities to identify and alert human analysts to threats, such as potential terrorist attacks or significant military movements. This capability will make critical warnings more timely, actionable, and relevant, allowing for more effective responses to emerging threats and hidden strategic opportunities.

Consider the example of Israel in January 2018 when its intelligence service, the Mossad, covertly broke into a secret Iranian facility and stole about 20 percent of the archives that detailed Iran's nuclear activities between 1999 to 2003.[1] According to Israeli officials, the Mossad collected some 55,000 pages of documents and a further 55,000 files stored on CDs, including photos and videos—and nearly all of it in Farsi.[2] Once obtained, the pressure from senior officials for detailed assessments of its contents and whether it pointed to an ongoing effort to build an Iranian bomb was immense, yet it took intelligence professionals several months to translate each page, review it by hand for relevant content, and incorporate this new information into assessments.

- With today's AI capabilities, the first two steps in that process — translation and highlighting relevant details — could have been accomplished within days, perhaps even hours.

[1] David Sanger and Ronen Bergman, "How Israel, In Dark of Night, Torched Its Way To Iran's Nuclear Secrets," New York Times. July 15, 2018

[2] The Iran Nuclear Archive: Impressions and Implications. The Belfer Center, Harvard University. April 2019

AI as A New National Security Challenge

While the potential is great, AI also poses significant new challenges for our National Security Enterprise. For one thing, a host of foreign countries — including several U.S. adversaries — are already investing heavily in AI for their own national security purposes. China, for instance, is expected to more than double its investment in AI to nearly $27 billion by 2026.[3] Moreover, while there is a great deal of attention being paid today to the creators of large, expensive-to-train foundation models, the presence of several capable so-called “open source” AI models – such as Meta’s LLAMA or Mistral’s 7B — means that speed at which this technology will become generally available will be very rapid. Unlike the advent of the atomic age, you will not need to be a well-resourced nation state to be able to benefit from AI technologies.

Therefore our intelligence services ***must devote additional resources and effort to ascertain what foreign competitors and non-state actors are doing to develop their own indigenous AI systems; and how they intend to employ them against us and our allies***.

- We’ve already seen evidence of AI being used to create believable misinformation, life-like videos and audio files that appear authentic, that are being used to push false narratives. But these same AI tools can be used to uncover sensitive U.S. military and intelligence operations, plan more sophisticated cyberattacks, and develop novel bioweapons.

- Looking ahead, ***defending our own “national security AIs” also will be crucially important***. As we grow more reliant on AI for “sense-making” and to drive decisions, we can ill afford to have malign foreign actors damaging or debilitating them. Our nation will need to equip its national security AIs with strong protections along the entire tech stack, including data, training weights, and algorithms.

AI, Intelligence, and Privacy

It is this Board’s mandate to focus on the implications of U.S. Government actions for civil liberties and privacy, and adoption of AI by the IC certainly poses some important new questions to be addressed. We should all read closely the unclassified details of

[3] Ben Wodecki, “China Set To More Than Double AI Spending by 2026.” Data Center Knowledge, 14 October 2022.

the White House's forthcoming National Security Memorandum when it is released later this month, as it likely will provide the initial framing of how the government thinks these questions should be properly answered. To my mind, those questions fall into one of two broad categories when it comes to ChatGPT-like large language generative AI models:

This first category is, what are the ***parameters that will guide whether the IC can make use of any particular model***? Obviously, there will be a security aspect to this; as I have said national security AIs probably will be regarded as vital national assets deserving of strong protections. And there should be a performance aspect; the IC should insist on high standards for accuracy and reliability. Delivering a threat assessment to the President that was prepared by an AI that may have hallucinated is not acceptable.

- But there's a more fundamental aspect to it. If leading-edge LLMs are basically trained off the Internet, which is composed mostly of US-derived information, how does this affect IC agencies' use of such models? Specifically, how can agencies utilize AI and remain compliant with Intelligence Community Directive 107 concerning privacy protections? Right now, I think different IC agencies are interpreting the rules differently.

The second category is, ***what will be non-acceptable uses of generative AI for the U.S. Intelligence Community***? As we try to figure out what are examples of "non-acceptable" uses, I expect we will go through a lengthy trial-and-error process informed mostly by "I'll know it when I see it"-type wisdom. Some restricted areas will be obvious; relying on AI systems alone to target suspected terrorists for kinetic strikes, for example. Other potential restrictions will be less obvious or in need of careful deliberation.

- For example, imagine a scenario in which a U.S. intelligence service proposes to contact another government and request that they detain a foreign national transiting their country based purely on the recommendation of a LLM AI model? What are the expectations for human review of that recommendation?
- Or more challenging: What if the AI detects what it assesses to be an imminent cyberattack that could occur any second. The AI says it "knows" exactly which U.S. computer systems to lockdown to thwart the attack. There is no time to gather policymakers for a meeting to decide the right course of action. Will the AI be granted any pre-authorization to mount a defense?

We will see if the new National Security Memorandum clarifies things or not, but I suspect we are embarked on a long journey to determine whether, and more importantly how, the IC uses AI to its advantage. I recognize the risks that this new technology poses. Nonetheless, I would urge the President, Congress, and this Board to not tie our IC's hands prematurely by reflexively imposing draconian restrictions against the use of AI as this would set us back in the tech competition with the PRC and other adversaries.

I am confident that we can mitigate the risks consistent with our national values while still taking maximum advantage of AI to safeguard our national interests and security. I know this is often easier said than done, but we can be sure our adversaries are prepared to use these technologies against us, so we must stay ahead.

Thank you and I look forward to your questions.