U.S. Senate AI Insight Forum
AI & National Security

Written Statement of Dr. Scott Philips
Chief Technology Officer, Vannevar Labs
December 6th, 2023

Thank you Leader Schumer, Senator Young, Senator Heinrich, and Senator Rounds for your leadership in holding this series of forums on artificial intelligence. Vannevar Labs is grateful for the opportunity to inform the US Senate about our work using artificial intelligence (AI) and machine learning (ML) as a component of our efforts to build software capabilities for national security.

My name is Scott Philips, and I am the Chief Technology Officer at Vannevar Labs. I lead a team of software engineers, machine learning engineers, and cybersecurity professionals who care deeply about building technology for national security missions. I have spent the last 20 years building AI capabilities for the defense and intelligence community. My PhD was funded in 2003 by the Office of Naval Research (ONR) to build machine learning technology that could identify Russian submarines in sonar data. After graduate school the US government was prioritizing counter-terrorism missions, so we adapted those AI algorithms to detect and track insurgents in overhead sensor feeds mounted on unmanned autonomous vehicles (UAVs). At the time, we were able to leverage massive improvements in AI for computer vision to solve big problems surrounding the safety and security of our forces in Iraq and Afghanistan.

Today, in the era of strategic competition, the problems are similar but also more complex and nuanced. In the Pacific alone, the U.S. has a wide range of ongoing activities connected to strategic competition including large force exercises, key leader engagements, conceal / reveal operations of new capability, and economic initiatives meant to change investment patterns. The big question is — are any of these activities moving the needle on our strategic priorities? How is the adversary perceiving our efforts? How are our allies and partners perceiving them? Are we contributing to the U.S. goals of achieving integrated deterrence or expanding access, basing, and overflight?

These are questions AI is uniquely suited to address. The answers exist, but not in traditional government-collected sensor feeds, such as from UAVs. They exist in the open source, spread across hundreds of countries in dozens of languages and in multiple formats (text, imagery, video). The challenge is compounded by a flood of misinformation attempting to convince our partners and allies that the U.S. is not a reliable partner. AI can help us peer through this fog of war to provide clarity, insight, and wisdom at the most critical times for our country.

Still, when we think about AI in national security, we tend to think about autonomous weapon systems. In my experience, AI in national security is instead best applied toward improving our ability to analyze and reason over large volumes of data to enable better, data-driven decisions from the tactical to the strategic. Domains like intelligence production and information operations are areas that can massively benefit from improved AI decision making without the safety risks associated with kinetic operations.

What should we consider when it comes to AI in defense?

Getting data right is critical.

Getting AI right means getting data right. In previous eras, the government had a monopoly on collecting data relevant to national security. Now, in a digital world, publicly and commercially available information are quickly becoming our dominant data sources for understanding the world. We need clear guidance on how to balance justifiable privacy concerns over the collection of this data with the tremendous value this data can provide our national security community. Due to historical rules, many of the units we work with are unsure if they are allowed to even analyze a local newspaper while on deployment without specific authorities or personnel qualifications.

The government should consider investing in "first party" collectors of this data—meaning commercial organizations that directly source mission-relevant information in the targeted way the government collects its own information. This can serve as a new, non-traditional form of sensors or reconnaissance in the digital environment. These first party collectors reduce concerns about incidental collection on US persons and other privacy issues that have cropped up in the past around "third party" collectors or data brokers that hoover up commercial data that may not be mission relevant or targeted.

Train like you fight.

Given uncertainties around AI's capabilities and deficiencies, there is a temptation to keep it in the lab until we can thoroughly evaluate the potential opportunities or harms. I couldn't disagree with this impulse more. We need to get these tools into the hands of the warfighter so they can experiment with novel concepts of employment, identify technology gaps, and feed back risks from real world use. When Vannevar partners with DoD users to solve hard problems, the lessons learned get incorporated into new techniques, tactics, and procedures that eventually change their warfighting doctrine – and that's a good thing. Congress needs to support efforts to quickly prototype and field operational AI/ML capabilities through the development of flexible programs that provide scale and velocity to reinforce successful efforts. I'm happy to provide specific examples in the closed session.

Encourage Defense Technology Startups.

The government has famously long acquisition timelines and regulatory compliance that make it difficult to work with. This reality prevents many companies and investors from entering the defense space. We should be thoughtful before adding additional compliance requirements for AI that limit new entrants from supporting our national defense. As an example, Vannevar Labs submitted a proposal for AI development in June 2022, it was endorsed by the commanding officer of the unit, was selected for award in February 2023, and still has not been contracted. Once contracted, the program goals include spending three years working towards an authority to operate (ATO) on a classified network. It's interesting to note at the time we submitted this AI/ML proposal, ChatGPT would not exist for another six months, and if our delivery schedule holds, the technology we are building will not be available on the desired network until at least 2027. We encourage Congress to be thoughtful as you consider additional AI-specific steps in the defense acquisition process.

Holistic AI Safety and Security.

Governments tend to view AI safety around academic benchmarks, such as, accuracy against a set of test data or error rates in a simulation environment. While valuable, these "AI in isolation" metrics don't tell you how an AI will perform in a real-world scenario. In the Department of Defense (DoD), AI is just one component of a larger system and used in complex warfighting environments. OpenAI made the right decision to do a wide release of ChatGPT in order to, as Sam Altman put it, "allow society to co-evolve with AI". We need to do the same with our military. We need to co-evolve our military tactics, techniques, and procedures in the context of training with these tools. Developing an AI literate workforce that knows when to trust AI, and when *not* to trust AI, is as important a safety issue as the rate of large language model (LLM) hallucination. Testing these technologies within the context of non-kinetic missions in the intelligence and information domains can also serve as an important proving ground for building trust and confidence. Informing these models with data from first party collectors mentioned above further reduces the risk that models generate responses that are not timely, factual, or mission relevant.

Countering China's use of AI.

As a nation, we should take China's stated goals for military applications of AI/ML seriously. China seeks to dominate AI in service of advancing their authoritarian governance model and has ambitions to use AI to reshape diplomatic, information, military, and economic systems to their own advantage. The Chinese military has unfettered compulsory access to any technology under development by Chinese industry and they have not hidden their ambition to dominate the military applications of AI.

In the information environment the impacts of AI can be particularly difficult to detect, attribute, and counter. The commander of the new Pacific Fleet Information Warfare Command Rear

Admiral Michael Vernazza said the following about the need to contest China in the information environment at a public forum in February of this year: *While the information age has been net positive, it has also provided malign actors numerous new outlets and mediums to spread disinformation, propaganda, and lies… malign actor nations in the information space rely on deniability and they seek to remain below the response threshold and achieve cumulative effects through seemingly minor actions*."[1]

Luckily, the same advances in artificial intelligence that enable our adversaries to sow doubt also give us the tools for defense. Identifying new strains of misinformation, characterizing its spread across dozens of island nations, and suggesting new courses of action is not just an interesting research project, it is executable today. The technology and capability exist. It just requires investments to integrate these tools across the larger defense enterprise.

Vannevar Labs is a next generation defense software company that uses artificial intelligence and machine learning to collect, translate, and exploit hard to access publicly available information (PAI) from foreign information environments to help the U.S. manage its relationship with strategic competitors like China and Russia. Vannevar Labs seamlessly integrates numerous AI/ML technologies to drive mission outcomes for our partners in the Department of Defense, including commercial, opensource, and bespoke models for translating, summarizing, and alerting across over 8000 data sources in 160 countries and 70 languages. Vannevar Labs' custom models are trained on hundreds of terabytes of data specifically curated to answer information requirements for our users across the Department of Defense. We believe connecting best-of-breed AI models to well scoped mission relevant data is the path to successful adoption of AI/ML for national security purposes.

[1] Pomerleau, M. (2023, February 16). *Here's what the New Information Warfare Command in the Pacific is doing*. DefenseScoop. https://defensescoop.com/2023/02/16/heres-what-the-new-information-warfare-command-in-the-pacific-is-doing/