TESTIMONY BEFORE THE
SENATE ARMED SERVICES SUBCOMMITTEE ON CYBERSECURITY

HEARING ON ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING
APPLICATIONS TO ENABLE CYBERSECURITY

April 19, 2023

Statement by Shyam Sankar
Chief Technology Officer, Palantir Technologies Inc.

Introduction

Chairman Manchin, Ranking Member Rounds, distinguished members of the subcommittee, thank you for the opportunity to discuss one of the most important subjects facing the U.S. Department of Defense and our nation: the effective and ethical deployment of artificial intelligence (AI) capabilities, including the large language models (LLMs) that have recently captured our collective attention, across the armed services and intelligence communities.

In February, I had the opportunity to visit Ukraine and witness the future of warfare.

By skillfully developing, integrating, and deploying AI-powered software on the battlefield, the Ukrainians have managed to effectively resist an adversary that by any conventional measure has a decisive advantage.

In addition to the bravery and ingenuity of Ukraine’s warfighters, I witnessed the incredible speed with which the Ukrainian defense forces were able to adopt, field, and scale new technological innovations.

While the traditional cycle of commercial innovation and government adoption for a novel technology can take years in the United States, the drive and focus of the leadership in Kyiv has significantly accelerated the country’s process for procuring and deploying new software on the battlefield, trimming adoption timelines from years and months to weeks and days.

It is clear that the future of warfare is upon us. The war in Ukraine has now provided critical lessons for improving the speed with which the U.S. government is able to adopt and deploy new technology at the pace required by the warfighter.

As a result, I welcome the opportunity to provide my perspective, working for a company whose software is on the front lines of the digital transformation of warfare, on both the benefits and risks of this novel and emerging set of AI capabilities, for the Department of

Defense, as well as to provide recommendations regarding the ways in which the U.S. military might most effectively harness the power of these advanced technologies while also mitigating their risks.

The Importance of AI and Defense

When appropriately used, AI has the capability to provide military leaders — at the strategic, operational, and tactical levels — with the ability to make decisions at greater speed and with greater confidence.

These technologies systematically augment the efficiency of warfighters on the ground. And there is no question that such technologies can help provide the advantage that the United States requires in order to deter its adversaries, and when necessary, to defeat them on the battlefield.

We are still only at the beginning of understanding the potential of these technologies for the military. The United States cannot run the risk of falling behind as a leader in this area, particularly to our adversaries, including China.

It is vital that we identify critical gaps in the Department of Defense's ability to acquire and field novel forms of AI, as well as aggressively expand the investments that are required to maintain America's technological edge.

The Current State of AI and Defense

The successful acquisition and application of AI capabilities raises significant technical issues, including the need to (1) track the provenance and lineage of data and models, (2) control for changes in versions of models as they are tested and upgraded, (3) provide a means of structuring data so that it reflects objects in the physical world and the relationships between them, (4) perform continuous testing and evaluation to bolster models against the inevitable impacts of entropy and brittleness, and (5) create a persistent and reliable audit trail to enable accountability and transparency.

We have learned from our own experience working with the Department of Defense that even though novel forms of AI are now actively deployed across the U.S. military, the foundational digital infrastructure required to support the sustained development of AI efforts across the armed services remains in its earliest stages.

Despite considerable progress, advances in the use of AI by the Department of Defense remain uneven across offices and branches of the military. At present, the vast majority of operational and strategic decisions are made based on a scattered assemblage of PowerPoint presentations, emails, and documents. Even the most basic retrospective analyses — to take stock of past decisions and outcomes, and to build on prior experience and knowledge — require analysts and warfighters to engage in tedious and inefficient workflows and processes.

This uneven landscape of technical advances alongside a structural reliance on legacy systems suggests that many areas of the Department of Defense still require a significant overhaul of their foundational data infrastructure before they can leverage more advanced AI capabilities.

The Army Vantage program is one example of the ways in which investing in modernization and digitalization efforts can lead to greater success and technological adoption in the long run.

The foundation of the Army Vantage program is a digital platform where data from across the U.S. Army is integrated and analyzed in a single pane of glass to help advance Army readiness, resilience, and operational decision-making. This open and interoperable platform provides a software layer on top of legacy Army and commercial off-the-shelf (COTS) systems and is available to individuals across all echelons of the Army, subject to their security approvals.

To date, this investment has allowed the U.S. Army to field an AI-enabled platform that supports tens of thousands of users and has demonstrated critical value to the Army by delivering operational capabilities.

The platform has saved the Army billions of dollars by leveraging algorithms to prioritize unliquidated obligation reviews, improved the health of the force by integrating critical risk data points to create the Commander's Risk Reduction Toolkit, which helps prevent self-harm among our troops, and provided in-theater decision support to commanders responding to crises in the Middle East and Europe.

We believe that Army Vantage provides a prime example of how the Department of Defense can pursue modernization that will establish a foundation for the use of next generation AI across the U.S. military in the coming years.

Given the pace with which America's near-peer competitors as well as other adversaries are advancing their own AI capabilities, we cannot delay the process of investing in our own armed services.

Time is not on our side. If the United States hopes to stay ahead of its adversaries, it must move beyond traditional contracting approaches that were built for hardware acquisition and accelerate the adoption of more agile acquisition methods that have been designed for the procurement of software.

Recommendations

Investment in Foundational Platforms & Infrastructure

First, to field AI that is both effective and sustainable in the long run, the Department of Defense must invest in foundational digital platforms and data infrastructure.

It is a mistake to think of AI capabilities as plug-and-play tools that simply work out of the box. The reality is more complicated. AI must be embedded within the context of an organization's broader technical infrastructure, which is required to make AI truly operational, as opposed to decorative or performative.

In practice, this means adopting digital infrastructure that supports the full life cycle of data and model management, providing tools for continuous testing and evaluation. It also means providing commercial capabilities for procuring, managing, curating, and securing large scale — and often highly sensitive — data streams that drive AI development and use.

There have been some significant efforts to invest in this space, most notably the Deputy Secretary of Defense's AI and Data Accelerator (ADA) initiative and the subsequent creation of the Chief Digital and Artificial Intelligence Office. Robust investments in this office and in the Department of Defense's Chief Information Office toward scaling existing, commercially enabled offerings, are critical to building the foundation of our future artificial intelligence capabilities.

Expansion of "Field-to-Learn" Programs

Second, we must continue to expand "field-to-learn" programs for AI.

Project Maven is the Department of Defense's most successful AI pathfinder program, in large part because of its iterative "field-to-learn" and "test-fix-test" approaches. AI is fielded to end-users and operators via workflows relevant to their missions, models are improved through iteration with operators in the field, and then the refined system is extended to larger groups over time.

This approach represents what technology supporting rapid experimentation looks like, and fortunately, Project Maven has developed an extensible infrastructure that can support an increasing set of operational AI capabilities across a number and growing set of domains.

Through ADA, AI isoperationally deployed across many Combatant Commands (COCOMs), including within CENTCOM, where experience in actual conflicts is the bedrock standard of the "field-to-learn" methodology. Future opportunities for "field-to-learn" AI programs include the Optionally Manned Fighting Vehicle (OMFV) program, whose focus is on building a vehicle based on an AI platform, with everything from autonomous and partially autonomous maneuvering capabilities, as well as improved targeting and drone control.

Adoption of Large Language Models (LLMs)

We believe that the Department of Defense should be aggressively experimenting, while adhering to responsible AI practices, to understand potential use cases and limitations of LLMs.

Early use cases for natural language processing capabilities and LLMs that are already proving valuable in the commercial world include code assist tools, using language models to create operational applications for rapid prototyping and experimentation, and improved semantic search for documents to assist subject matter experts in finding the information they need. Future applications should include use in wargaming, creative assistants for operational planning, and faster battle damage assessments.

Many LLM use cases are going to require classified models trained on Department of Defense data and problem sets. The U.S. military should build off of models developed in the commercial world and trained on Department of Defense and proprietary data, to power future military systems. Joint All Domain Command and Control (JADC2) development provides an opportunity to test new warfighting concepts for decision-making that rely on LLMs, but these models should be available for broad integration in other programs so that our most important problems benefit from our most advanced AI technology.

Lower Barriers for Commercial Technical Innovation

Third, in order to leverage the value of technology in support national defense, the U.S. Congress and the Department of Defense should lower barriers to entry for America's most innovative firms.

I believe that America's greatest advantage over its adversaries is the power and sophistication of the software that this country produces. But America cannot exercise its software advantage if those who are most adept in providing it are unable to participate in the defense innovation ecosystem.

In order for the Department of Defense should grow more comfortable using software-specific acquisition authorities and Other Transaction Authorities (OTAs), it must simplify and accelerate the Authority to Operate (ATO) process.

Too often defense industry giants and incumbents are awarded contracts and tasked with projects that they will never be able to complete.

The government needs to hold them accountable for their lack of productivity and results. One way to do this is to invite more competition from those non-traditional firms and start-ups that are ready and willing to help the United States advance its AI capabilities.

The existing congressionally-mandated Commission on Planning, Programming, Budgeting, and Execution Reform is a welcome endeavor.

Advancing Responsible and Ethical AI

Fourth, the United States must take the lead on building a regulatory and ethical framework for the responsible use of AI in the defense context. If we do not set the tone and the rules, our adversaries will.

Our recommendations for guiding principles, both in and out of the defense context, include:

- *AI technologies need to be understood in their operational and systems context.* As a software company, we believe that it is critical to develop software and systems that are informed by operational realities and reflect the constraints and limitations — technological, procedural, and normative — that warfighters face in the field.

- *AI capabilities should be oriented towards addressing human concerns and outcomes.* The best technology solutions must augment rather than replace human intelligence.

- *Ethical AI goes hand-in-hand with effective AI*. It is not only an ethical imperative that AI innovation should be compatible with fundamental rights concerns, as well as domestic and international law (including international humanitarian law), but it is also the case that the most effective AI technologies are often built with principles of responsible operation and use embedded by design.

Effective AI should also enable responsible warfighting that reinforces principles of national law, military doctrine, and international humanitarian law to help ensure that our defense forces never lose sight of the values we are fighting to preserve.

Leverage Existing Commercial Technology

Finally, we believe that the Department of Defense must recognize that while there are some cases where it makes sense to build in-house, it is more prudent to buy AI capabilities from the commercial sector.

The bleeding edge of AI development is happening in America's robust marketplace of commercial firms. Instead of the government insisting on building in-house (which stands in direct competition with American businesses), or itself trying to serve as a systems integrator, the choice to buy commercial solutions will lead to a quicker, cheaper, sustainable, and more effective advancement of AI capabilities for America's warfighters.

Furthermore, the acquisition of commercially available AI capabilities will allow the Department of Defense to progress to the "field-to-learn" stage of AI development from the start, instead of waiting years to develop certain capabilities in-house.

I would add a final call to arms, not to the U.S. government, but to American technology companies in Silicon Valley and elsewhere.

We, the technology industry, have a debt to the American people and the free and liberal society that supports us. As a result, we owe it to consumers not to build products that are extractive and predatory. We have an obligation to build products that strengthen individuals and society at large, and we must be part of a system that builds a strong economy for the American worker and democratic principles.

Conclusion

In the late 1930s, European refugees warned of Germany's advances in developing atomic weapons, and with the support of individuals such as Robert Oppenheimer and Albert Einstein, the Manhattan Project was born.

When the Sputnik satellite was launched in 1957, just decades later, America put a man on the moon. When a highly contagious virus ravaged the world and killed tens of thousands of people each day, America's best scientists created effective vaccines and partnered with the military to deliver them in record time, through Operation Warp Speed.

We are now at another inflection point.

Without fully embracing the power of advanced software and AI, the United States runs a real risk of falling behind its adversaries. AI-enabled warfighting is not about large weapons systems that take decades and billions of dollars to develop, but rather about having the systems in place — both institutionally and technologically — to support rapid, iterative experimentation and deployment.

The creation of such a system, and especially one that is ethical and reliable, will require a concerted and joint public-private effort. It is for this reason that I am honored to testify before this subcommittee today, and I look forward to working with colleagues in the U.S. government as well as industry to bring the best technology possible to members of our armed services.

We must invest, build, and scale this new technology as soon as possible.

Thank you, and I look forward to your questions.