

**THE STATE OF ARTIFICIAL INTELLIGENCE AND
MACHINE LEARNING APPLICATIONS TO IM-
PROVE DEPARTMENT OF DEFENSE OPERATIONS**

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY

OF THE

COMMITTEE ON ARMED SERVICES

UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

—————
APRIL 19, 2023
—————

Printed for the use of the Committee on Armed Services



Available via <http://www.govinfo.gov>

—————
U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON ARMED SERVICES

JACK REED, Rhode Island, *Chairman*

JEANNE SHAHEEN, New Hampshire	ROGER F. WICKER, Mississippi
KIRSTEN E. GILLIBRAND, New York	DEB FISCHER, Nebraska
RICHARD BLUMENTHAL, Connecticut	TOM COTTON, Arkansas
MAZIE K. HIRONO, Hawaii	MIKE ROUNDS, South Dakota
TIM KAINÉ, Virginia	JONI ERNST, Iowa
ANGUS S. KING, Jr., Maine	DAN SULLIVAN, Alaska
ELIZABETH WARREN, Massachusetts	KEVIN CRAMER, North Dakota
GARY C. PETERS, Michigan	RICK SCOTT, Florida
JOE MANCHIN III, West Virginia	TOMMY TUBERVILLE, Alabama
TAMMY DUCKWORTH, Illinois	MARKWAYNE MULLIN, Oklahoma
JACKY ROSEN, Nevada	TED BUDD, North Carolina
MARK KELLY, Arizona	ERIC SCHMITT, Missouri

ELIZABETH L. KING, *Staff Director*
JOHN P. KEAST, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY

JOE MANCHIN III, West Virginia, *Chairman*

KIRSTEN E. GILLIBRAND, New York	MIKE ROUNDS, South Dakota
GARY C. PETERS, Michigan	JONI ERNST, Iowa
TAMMY DUCKWORTH, Illinois	TED BUDD, North Carolina
JACKY ROSEN, Nevada	ERIC SCHMITT, Missouri

CONTENTS

APRIL 19, 2023

	Page
THE STATE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING APPLICATIONS TO IMPROVE DEPARTMENT OF DEFENSE OPERATIONS	1
MEMBER STATEMENTS	
Statement of Senator Joe Manchin	1
Statement of Senator Mike Rounds	3
WITNESS STATEMENTS	
Matheny, Jason G., President and Chief Executive Officer, Rand Corporation and Commissioner, National Security Commission on Artificial Intelligence	4
Sankar, Shyam, Chief Technology Officer and Executive Vice President, Palantir	7
Lospinoso, Josh, Co-Founder and Chief Executive Officer, Shift5	12

**THE STATE OF ARTIFICIAL INTELLIGENCE
AND MACHINE LEARNING APPLICATIONS
TO IMPROVE DEPARTMENT OF DEFENSE
OPERATIONS**

WEDNESDAY, APRIL 19, 2023

UNITED STATES SENATE,
SUBCOMMITTEE ON CYBERSECURITY,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The Subcommittee met, pursuant to notice, at 9:32 a.m., in room 222, Russell Senate Office Building, Senator Joe Manchin (Chairman of the Subcommittee) presiding.

Subcommittee Members present: Senators Manchin, Peters, Rosen, Rounds, and Schmitt.

OPENING STATEMENT OF SENATOR JOE MANCHIN

Senator MANCHIN. Committee will come to order. Thank you all for coming. I appreciate it very much. The subcommittee meets this morning to receive testimony from outside experts and industry leaders on developments in artificial intelligence and machine learning in the private sector that may have benefits for the Department of Defense. Our witnesses today are Dr. Jason Matheny.

Dr. Matheny is President and Chief Executive Officer (CEO) of RAND Corporation and Commissioner of the National Security Commission on Artificial Intelligence (AI). We have Mr. Shyam Sankar—okay, thank you, sir. Chief Technology Officer of Palantir.

I knew your CEO very well, and Mr. Josh Lospinoso, did I get that right? Good. Chief Executive Officer of Shift5. We welcome our witnesses to the Committee and thank them for their willingness to share their insights with us. This Subcommittee has been keenly interested in the Department of Defense's (DOD) approach to adopting and integrating artificial intelligence, or AI, into the Department of Defense processes.

We recognize the opportunity that AI represents to radically influence how DOD fights and defends and operates, which was the chief reason we supported the establishment of the National Security Commission on Artificial Intelligence in the 2019 National Defense Authorization Act (NDAA).

The results from the Commission, as well as the seeming overnight success of generative AI systems like ChatGPT and DALL-E have reinforced our instincts that AI will be a game changer for DOD, the United States, and our industry partners. However, say—to stay ahead of our potential adversaries, we also have to be

working at a speed and scale that keeps us ahead of any progress that they are currently making.

To do that, we need to identify key technologies and integrate them into our systems and processes faster than they can. That means harnessing innovation in the commercial marketplace to gain speed, but also reduce barriers for those tools to be implemented within DOD for the benefit of our warfighters. Some of the challenges we are facing are technical.

While user friendliness and reliability are key attributes needed for commercial and defense markets for the Department, the applications deployed must be more secure and trusted. Meaning we understand the logic behind its algorithms, so it cannot be used in unintended ways, and have more rigorous policy enforcement mechanisms to prevent misuse or unintended use.

Because we have heard much in the press on debates over potential biases and algorithms, I think it would be helpful if the witnesses can share their thoughts on what is happening on the commercial side to identify and remedy the bias in their algorithm development.

How do you all bake this consideration into your software development process is the question we would like to have answered. Also, with the discussions on ethical implications of AI, we would appreciate your thoughts on how you think about this from your corporate perspective, but also how do you think the Pentagon and U.S. Government should be approaching these debates?

Last, I would like to ask our witnesses to touch on what I believe is DOD's most crucial resource in AI development, data. We collect vast quantities of data, which is the knowledge base for any artificial intelligence, but do regularly run into issues of ownership and management of that data.

I believe it is clear to the Subcommittee that data should be agnostic, if it is collected through DOD mission. The Pentagon owns it and should be able to use it across the entirety of our systems. I would also like to point to some of the progress that is being made, especially within the Department.

I mentioned earlier the National Security Commission on Artificial Intelligence, they did a fantastic job of providing a framework for us to think about these issues and made some great recommendations, many of which we have enacted in previous NDAAAs. But there are still others that haven't been implemented that we should be considering.

Finally, I would like to commend the Department for the progress in establishing the Chief Data and Artificial Intelligence Officer, or CDAO. In short—and in very short time they have established themselves to make positive progress in both sides of the job, improving the Department's data and pushing adoption of AI tools.

There too, we still have progress. We can do better. Position DOD to deal with the future security challenges that we know they are going to face. With that, I turn to my friend Senator Rounds, for any remarks he may have.

STATEMENT OF SENATOR MIKE ROUNDS

Senator ROUNDS. Well, thank you, Senator Manchin, for convening this very important hearing today. I think you will find that our opening statements are going to be very similar in nature.

We really do appreciate all of you coming and participating in this with us today. In 2018, the Department of Defense published its foundational strategy on artificial intelligence.

The strategy predicted that AI was poised to change the character of the future battlefield and the pace of threats that we must face. Nearly 5 years later, that future battlefield is here.

Breakthroughs in AI research and development are transforming the military's capabilities and are reshaping the character of warfare across all warfighting domains.

The adoption of AI technologies in the cyber domain has been particularly transformative, as intelligent systems are empowering department personnel to analyze network patterns across thousands of data points in real time and expand their situational awareness on the digital battlefield.

Through increased visibility into network assets, the military cyber operators are able to identify anomalies, detect threats, patch vulnerabilities, and mitigate cyber-attacks across the information enterprise more efficiently.

AI tools are also being leveraged to prioritize risks, automate response actions, and extend DOD's ability to protect its digital assets beyond the capacity and reach of human security defenses.

AI's ability to make inferences, strengthen access control measures, and streamline threat hunting processes are among the other features of this technology that are helping to enhance our defensive posture throughout the cyber environment.

Despite the benefits of artificial intelligence, we cannot lose sight of how this powerful technology is changing the cyber battlefield for our adversaries as well.

AI presents a new attack surface for foreign adversaries and cyber criminals to exploit. There is no doubt that malicious actors are seeking new ways to attack our critical infrastructure, steal sensitive information, and spread malware and other cyber threats through AI systems.

Mitigating an adversarial AI will be key to winning the race for global AI leadership and securing the United States' technological dominance in this important field. Today's hearing is an opportunity to discuss the State of AI and machine learning applications to support cybersecurity.

I look forward to witnesses discussing AI product and service offerings on the market today, and how they are protecting commercial organizations and digital systems from cyber threats.

I also hope witnesses will discuss the regulatory landscape, guiding AI innovation both domestically and abroad, as well as how Congress can appropriately balance the demand for more AI research and innovation amid calls to pause its development due to transparency, accountability, and safety concerns.

To defend against evolving threats in cyberspace, I would appreciate the witnesses discussing promising gains in AI research, identifiable limitations or gaps in the technology, and how the United

States can outcompete large and sustained investments into AI applications by our foreign competitors.

I would also appreciate witnesses discussing how the commercial sector is protecting its data repositories and algorithms to preserve the integrity of AI systems. I look forward to a discussion on all of these important matters. Thank you again to our witnesses for appearing today. Senator Manchin.

Senator MANCHIN. Thank you, Senator Rounds. Now we are going to turn to our witnesses. First we have Dr. Jason Matheny for his opening statement.

STATEMENT OF JASON G. MATHENY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, RAND CORPORATION AND COMMISSIONER, NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

Dr. MATHENY. Thank you, Chairman Manchin, Ranking Member Rounds, and Senator Schmitt. Thanks for the opportunity to testify today.

I am the President and CEO of the RAND Corporation, a non-profit, nonpartisan research organization. Before RAND, I served in the White House National Security Council and the Office of Science Technology Policy as a Commissioner on the National Security Commission on Artificial Intelligence.

For the past 75 years, RAND has conducted research in support of U.S. National Security, and we currently manage four federally funded research and development centers for the Federal Government. Including one for the Secretary of Defense, one for the Secretary of the Air Force, one for the Secretary of the Army, and one for the Secretary of Homeland Security.

Today, I am going to focus my comments on how DOD can best ensure that progress in AI benefits U.S. National Security instead of degrading it. Among a broad set of technologies, AI really stands out both for its rate of progress and for its scope of potential applications. It holds the potential to broadly transform entire industries, including ones that are critical to our future economic competitiveness and our National Security.

Integrating AI into our National Security plans poses special challenges for several reasons. First, the technologies are driven by commercial entities that are frequently outside of our National Security frameworks.

Second, the technologies are advancing quickly, typically outpacing policies and organizational reforms within Government. Assessments of the technologies require expertise that is concentrated in the private sector, and that has rarely been used for National Security.

The technologies lack conventional intelligence signatures that distinguish benign from malicious use. Although the United States is currently the global leader in AI, this may change as China seeks to become the world's primary AI innovation center by 2030, an explicit goal of China's AI national strategy. In addition, both China and Russia are pursuing militarized AI technologies, intensifying the challenges that I just mentioned.

In response, I will highlight a few sets of actions that DOD could take. The first is to ensure that DOD cybersecurity strategies and

cyber red team activities track developments in AI that could affect cyber defense and cyber offense, such as the automated development of cyber weapons, or at least development that requires much shorter timelines.

Second, to prevent bad actors from having access to advanced AI systems, first, ensure strong expert controls of leading-edge AI chips and chipmaking equipment, while licensing benign uses of chips that can be remotely throttled as needed.

Second, use Defense Production Act authorities to require that companies report the development or distribution of large computing clusters, training runs, and trained models above a certain size. Third, including in DOD contracts with cloud computing providers a requirement that they employ know your customer screening for all customers before training large AI models.

Fourth, including DOD contracts with AI developers know your customer screening as well as cybersecurity requirements to prevent the theft of large AI models, so that our competitors aren't stealing the technologies that we are actually building.

Third, work with the intelligence community to significantly expand the collection and analysis of information on key foreign, public and private sector actors in adversary states, including those foreign public and private entities that are making headway in AI and in AI relevant computing, their infrastructure, their investments, their capabilities, their supply chains of tools, material, and especially talent.

Strengthen DOD's institutional capacity for such activities by creating new partnerships and information sharing agreements among U.S. and allied government agencies, academic labs, and industrial firms, and by recruiting private sector AI experts to serve in the Government on short term or part time appointments.

Fourth and last, invest in potential moonshots for AI security, including microelectronic controls that are embedded in AI chips to prevent the development of large AI models without security safeguards.

Second, generalizable approaches to evaluate the security and safety of AI systems before they are deployed. I thank the Committee for the opportunity to testify and look forward to your questions.

[The prepared statement of Dr. Jason Matheny follows:]

PREPARED STATEMENT BY JASON MATHENY^{1 2}

Chairman Manchin, Ranking Member Rounds, and Members of the Committee: Good morning, and thank you for the opportunity to testify today. I'm the president and CEO of RAND, a nonprofit and nonpartisan research organization. Before RAND, I served in the White House National Security Council and Office of Science and Technology Policy, as a commissioner on the National Security Commission on Artificial Intelligence, as assistant director of national intelligence, and as director of the Intelligence Advanced Research Projects Activity, which develops advanced technologies for the U.S. intelligence community.

¹The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of the RAND Corporation or any of the sponsors of its research.

²The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND's mission is enabled through its core values of quality and objectivity and its commitment to in-

For the past 75 years, RAND has conducted research in support of U.S. national security, and we currently manage four federally funded research and development centers (FFRDCs) for the Federal Government: one for the Department of Homeland Security (DHS) and three for the Department of Defense (DOD). Today, I'll focus my comments on how DOD can best ensure that progress in artificial intelligence (AI) benefits U.S. national security instead of degrading it.

Among a broad set of technologies, AI stands out for both its rate of progress and its scope of applications. AI holds the potential to broadly transform entire industries, including ones critical to our future economic competitiveness and our national security. Integrating AI into our national security plans poses special challenges for several reasons:

- The technologies are driven by commercial entities that are frequently outside our national security frameworks.
- The technologies are advancing quickly, typically outpacing policies and organizational reforms within government.
- Assessments of the technologies require expertise that is concentrated in the private sector and that has rarely been used for national security.
- The technologies lack conventional intelligence signatures that distinguish benign from malicious use.

The United States is currently the global leader in AI;³ however, this may change as the People's Republic of China seeks to become the world's primary AI innovation center by 2030—an explicit goal of China's AI national strategy.⁴ In addition, both China and Russia are pursuing militarized AI technologies,⁵ intensifying the challenges I just outlined. In response, I will highlight four sets of actions that DOD could take:

1. Ensure that DOD cybersecurity strategies and cyber Red team activities track developments in AI that could affect cyber defense and cyber offense, such as the automated development of cyber weapons.
2. To prevent bad actors from having access to advanced AI systems, (1) ensure strong export controls of leading-edge AI chips and chip-making equipment while licensing benign uses of chips that can be remotely throttled if need be; (2) use Defense Production Act authorities to require companies to report the development or distribution of large AI computing clusters, training runs, and trained models (e.g. >1,000 AI chips, >1027 bit operations, and >100 billion parameters, respectively); (3) include in DOD contracts with cloud-computing providers a requirement that they employ “know your customer” screening for all customers before training large AI models; and (4) include in DOD contracts with AI developers “know your customer” screening, as well as strong cybersecurity requirements to prevent the theft of large AI models.
3. Work with the intelligence community to significantly expand the collection and analysis of information on key foreign public-and private-sector actors in adversary states involved in AI, including assessments of key foreign public and private entities; their infrastructure, investments, and capabilities; and their supply chains of tools, material, and talent. Strengthen DOD's institutional capacity for such activities by (1) creating new partnerships and information-sharing agreements among U.S. and allied government agencies, academic labs, and industrial firms and (2) recruiting private-sector AI experts to serve in the government on short-term or part-time appointments.

tegrity and ethical behavior. RAND subjects its research publications to a robust and exacting quality-assurance process; avoids financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursues transparency through the open publication of research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. This testimony is not a research publication, but witnesses affiliated with RAND routinely draw on relevant research conducted in the organization.

³Although there are many ways to measure this, the Stanford Global AI Vibrancy Tool has consistently ranked the United States at the top. See Stanford University, “Global AI Vibrance Tool: Who's Leading the Global AI Race?” undated, <https://aiindex.stanford.edu/vibrancy/>.

⁴Graham Webster, Rogier Creemers, Elsa Kania, and Paul Triolo, “Full Translation: China's New Generation Artificial Intelligence Development Plan,” DigiChina, August 1, 2017, <https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>.

⁵Forrest E. Morgan, Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly Klima, and Derek Grossman, Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World, RAND Corporation, RR-3139-AF, 2020, <https://www.rand.org/pubs/research-reports/RR3139-1.html>.

4. Invest in potential moon shots for AI security, including (1) microelectronic controls embedded in AI chips to prevent the development of large AI models without security safeguards and (2) generalizable approaches to evaluate the security and safety of AI systems before they are deployed.

I thank the Committee for the opportunity to testify, and I look forward to your questions.

Senator MANCHIN. Thank you, and Mr. Sankar.

**STATEMENT OF SHYAM SANKAR, CHIEF TECHNOLOGY
OFFICER AND EXECUTIVE VICE PRESIDENT, PALANTIR**

Mr. SANKAR. Chairman Manchin, Ranking Member Rounds, Senator Schmitt, thank you for the opportunity to discuss one of the most important subjects facing both the Department of Defense and our Nation at large, the effective and ethical application and integration of artificial intelligence with our armed services.

This past February, I had the opportunity to visit Ukraine and witness the incredible speed with which the Ukrainian forces were able to field, learn, and win with AI on the battlefield. While the cycle of commercial innovation and Government adoption can take years in the United States, they were doing it in days in Ukraine.

So really, the future has already arrived, it is just not evenly distributed. In that future, AI rewrites our roadmaps. It changes everything. We can either choose to accept that disruption and drive that change, or we can get disrupted by defending against it. Because the future is already here, we need to act with speed and conviction. If I can impart one message today, is that we are facing a moment in which existing roadmaps and systems are insufficient.

We must completely rethink what we are building and how we are building it. Software and AI will shape everything, even toasters, but most certainly tanks. To succeed, we need to cut through the existing ways we organize and procure weapons systems and begin with software and AI first.

This will be disruptive and emotional. Many incumbents in Government will be affected and they will feel threatened and dislocated. Many careers that have been built on mature technologies, weapons systems and platforms will also be affected. Fortunately, with the right leadership, our country is amongst the few that can turn on a dime and do so at scale. Because the alternative should be unthinkable.

We must do the right thing, the hard thing here. As we begin this journey, I would like to offer the Subcommittee the following recommendations. First, the only way to overcome the intense emotional barriers to this wholesale reinvention is to adopt and embrace a field to learn to win model.

We should field AI to mission users and operational workflows at the earliest possible moment, and then continuously improve these models through iteration with operators in the daily deterrence of our enemies and the defense of the Nation. This is the technological equivalent of throwing ourselves off the deep end.

In the case of AI adoption, it is the only way to learn how to swim and win in this critical race. Second, the only way the Department of Defense will be able to employ world class AI with field to learn to win methods is if it overcomes the current market failures. An entire industry of commercial providers stands ready

to support the defense community, but they must often stand idle while the Government insists on starting from scratch.

America's greatest advantage over its adversaries is its software and its culture of innovation. Even our allies are envious of American technology companies and the prosperity that they have brought to our Nation. But America cannot exercise its software advantage unless those who are most adept at providing are able to bring their expertise and innovation to bear on these issues of national importance.

For example, if there was a need to use any of the cutting-edge large language models on a secret or top-secret network, today we cannot. This is a massive market failure. With a mere 10th of a percent of the Department's budget, we could bring cutting edge commercial innovation to our warfighters.

Today, I can give AVUS [Augmented Visualization of Underground Services] and AIG [Artificial Intelligence Group] more advanced AI than I can bring the Army and the Air Force. If we want to effectively deter those that threaten U.S. interests, we must spend at least 5 percent of our budget on capabilities that will terrify our adversaries. In the late 1960s, 95 percent of all integrated circuits were sold to the U.S. Government.

The Government was the first and largest customer, and it benefited directly from American innovation and ingenuity. The U.S. should aspire to recreate this dynamic with AI. Finally, these recommendations will only be successful if the United States continues to lead in building a regulatory and ethical framework for the use of responsible AI in the defense context.

We cannot cede this leadership to the illiberal value structures of our adversaries. Our allies are certainly watching. This is not an exercise for academics. It is about addressing directly real-world problems in real time.

Today we are at an inflection point. AI will define the success of every commercial and Government organization. Its development will define the prosperity of our Nation, and its adoption in the department will defend our country. I thank you, and I look forward to your questions.

[The prepared statement of Mr. Shyam Sankar follows:]

PREPARED STATEMENT BY SHYAM SANKAR

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. 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 decisionmaking. 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 is operationally 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 decisionmaking 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 startups 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 toward 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 1930's, 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.

Senator MANCHIN. Dr. Lospinoso.

STATEMENT OF JOSH LOSPINOSO, CO-FOUNDER AND CHIEF EXECUTIVE OFFICER, SHIFT5

Dr. LOSPINOSO. Thank you, Chairman. Chairman Manchin, Ranking Member Rounds, member of the subcommittee, it is my honor to have the opportunity to testify before you today on the State of artificial intelligence and machine learning applications to improve Department of Defense operations.

While AI research is by now many decades old, the field has accelerated at a blistering pace. From ChatGPT to self-driving cars, recent AI powered technologies have again captured the public imagination. I commend the Subcommittee for treating this accelerating development with renewed urgency.

In 2021, the National Security Commission on Artificial Intelligence (NSCAI) message was clear. If trends continue, China will surpass us within a decade. This Subcommittee has asked whether we have made progress toward the NSCAI's recommendations, what gaps exist, and where policy is impeded.

In this testimony, I want to bring attention to two facts about today's military weapons systems, AI and cybersecurity. Fact number 1, most major weapons systems are not AI ready. As data scientists are quick to say, garbage in makes garbage out.

Data allows us to investigate, train, monitor novel AI enabled technologies, but without high quality data, we cannot build effective AI systems. Unfortunately, today the DOD struggles to liberate even the simplest data streams from our weapon systems. These machines are talking, but the DOD is unable to hear them.

We cannot employ AI enabled technologies without great data. This requires taking seriously the difficult, unglamorous work of laying strong foundations, clean, labeled, enriched, comprehensive data, sound, simple, decentralized, scalable data architectures, and

straightforward, unambiguous metrics for measuring AI empowered systems' effectiveness.

America's weapon systems are simply not AI ready. While the Department of Defense's intention is to integrate and employ AI capabilities across the Joint Force, the weapons systems themselves are incapable of hosting them.

We must implement solid, scalable edge computing. We need to enable full tech data collection at the edge. We must solve the operational challenge of transferring terabytes of data from the field to the cloud, making them available to the AI enabled technologies they will fuel.

Fact number 2, the DOD cannot solve weapons systems cybersecurity without artificial intelligence. Without AI, the DOD will never be able to keep these weapon systems cyber secure. It has made little progress, unfortunately, addressing the perils identified in the Government Accountability Office's 2018 report on weapons systems' cybersecurity.

The DOD spends trillions of dollars fielding weapon systems. Each one contains dozens, sometimes hundreds, of special purpose computers that perform every conceivable function on these platforms, from the control surfaces on an aircraft to the data radios on submarines. These systems are profoundly digital.

Unlike modern IT systems, built with zero trust architectures, these weapon systems were built with blind faith architectures. The DOD needs AI powered capabilities to detect anomalies and prevent cybersecurity intrusions on these platforms.

The NSCAI is right, if we don't act now, China's goal of surpassing us will be realized. Major weapon system programs, both old and new, need funding and requirements to make them AI ready.

The good news is that between industry, academia, and Government, solutions to these challenges exist today. I look forward to discussing these matters with you and continuing to support the warfighter. Thank you, Chairman Manchin, Ranking Member Rounds.

[The prepared statement of Dr. Lospinoso follows:]

PREPARED STATEMENT BY DR. JOSH LOSPINOSO

Chairman Manchin, Ranking Member Rounds, Members of the Subcommittee, it is my honor to have the opportunity to testify before you today on the State of Artificial Intelligence and Machine Learning applications to improve Department of Defense operations.

While AI research is well over 60 years old, development seems to be accelerating at a dizzying pace. Recent AI-powered technologies ranging from ChatGPT to self-driving cars have again captured the public imagination. The subcommittee is correct to treat this accelerating development with renewed urgency. Additionally, given the DOD's foundational role in artificial intelligence research, it's fitting that the National Security Commission on Artificial Intelligence has taken up the challenge of considering how the U.S. can continue taking a central role in AI, responsibly employ AI for national security and defense, and protect against AI threats.

In this testimony, I want to bring to the subcommittee's attention two key facts about our weapon systems, AI, and cybersecurity:

1. Most major weapon systems are not AI ready
2. We cannot solve weapon system cybersecurity without AI

Today, the Department of Defense lacks the ability to collect, translate, enrich, store, and process weapon system data. Without these basic, fundamental elements, our major weapon systems cannot benefit from AI-powered technologies including

cybersecurity, maintenance, and operational applications. They are and will continue to be stuck in the last century, and there is a real risk that our adversaries will leapfrog over us as a result.

The NSCAI made two important claims: (a) AI will exceed humans in a wide range of tasks, and that this will have world-altering impacts; (b) that AI wielded by our adversaries, especially China, will challenge America's technological predominance.

I wish I could disagree, but I wholeheartedly share the NSCAI's convictions. I would like to take the opportunity to emphasize and sharpen several key recommendations within the NSCAI report: manage risks associated with AI-enabled and autonomous weapons; establish justified confidence in AI systems; and present a democratic model of AI use.

Most major weapon systems are not AI ready

As data scientists are quick to say, "garbage in makes garbage out." Data allows us to investigate, train, and monitor novel AI-enabled techniques. Without high-quality data, we cannot build effective AI systems.

If military weapon systems are going to benefit from the rapid expansion of AI-power technology, Congress must levy requirements for every major weapon system that they collect, translate, enrich, and disseminate their data. These systems are designed with nervous systems that carry tremendous volumes of extremely valuable data. We must extract this data and make it broadly available across the Department to achieve the four top priorities outlined by the 2022 National Defense Strategy. Congress must also fund the requirements. This funding should go toward procuring readily available technology solutions across industry, not to merely study the problem, but to address the problem. This is how we will deter or win the next major conflict. We cannot wait a decade.

AI-powered technology is only as good as the data used to train it. Getting this wrong on weapon systems could put the warfighter at risk or result in mission failure. Today, the Department of Defense does not have anywhere near sufficient access to weapon system data. We do not—and in some cases due to contractual obligations, the Department cannot—extract this data that feeds and enables the AI capabilities we will need to maintain our competitive edge. The Department of Defense must be empowered to holistically collect, assess, and manage data particular to those capabilities responsible for the defense of the Homeland. Ensuring that the Department not just has access to weapon systems data but can own that data will be a paradigm shift in the way the Department of Defense can truly assess total formation readiness. Enabled by AI technologies, commanders/operators/maintainers must have unparalleled visibility into not just the platforms but the fleets of weapon systems—without which, JADC2 cannot be achieved.

The DOD and the U.S. have played a formative role in advancing the field of AI. The NSCAI's report provides a roadmap for how the U.S. can retain AI preeminence, how the DOD must prepare for AI's potential impact on modern warfare, and how the world order could easily change if we misstep.

Each of these recommendations require the difficult, unglamorous work of laying strong foundations: clean, labeled, enriched, comprehensive data; sound, simple, decentralized, scalable data architectures; and straightforward, unambiguous metrics for measuring AI-empowered systems' effectiveness. Ask data scientists where they spend most of their time, and you'll hear that it's 90 percent data engineering, data cleaning, and data shaping. Obtaining and preparing the right data for a particular AI application is, by a wide margin, the least appreciated and resourced part of the process. Without robust, pristine, well-curated data sets, we must significantly reduce our expectations about the efficacy of AI applications built without this foundation.

I believe that three of the reports key recommendations—managing risks associated with AI-enabled weapons, establishing justified confidence in AI systems, and presenting a democratic model of AI use—require the unglamorous but essential work of laying strong foundations. This involves clean, labeled, enriched, and comprehensive data, sound and scalable data architectures, and straightforward and unambiguous metrics for measuring AI system effectiveness. This foundational work is crucial in ensuring weapon system cybersecurity, and the proposed solutions need to be implemented through funding and requirements. Ultimately, the successful deployment of AI in national security and defense requires a collaborative effort among government, academia, and industry to lay the groundwork and build on the progress made so far.

We cannot address weapon system cybersecurity without AI

As evidenced by the NCSAI report's length—over 750 pages—defense's role in AI is an enormous topic. I'd like to focus your attention on one specific and extremely consequential AI-enabled technology of great importance to the warfighter: weapon system cybersecurity. The Fiscal Year 2016 NDAA Section 1647 required DOD to complete cybersecurity vulnerability assessments for individual weapon systems. My colleagues and I spent considerable time studying these systems, and what we found unsettled us deeply. By comparison to weapon systems, IT systems like cell phones seem like impregnable fortresses. The Government Accountability Office arrived at the same conclusions, and in 2018 published its sobering "Weapon Systems Cybersecurity" report.

The DOD spends trillions of dollars fielding major weapon systems. Each one contains dozens—sometimes hundreds—of special purpose computers that perform every conceivable function. From the control surfaces on an aircraft to data radios on submarines, these systems are highly digitized. This digitization happened gradually over the latter half of the 20th century. Modern weapon systems are both profoundly digitized and highly interconnected. Many have radio frequency connections including to satellites and other weapon systems. Virtually all systems interconnect with IT systems such as maintenance laptops for routine upkeep. Some older systems were designed with the assumption that they would remain air gapped once they rolled off the assembly line. This assumption simply no longer holds in the modern military.

It is deeply unfortunate that we never architected cybersecurity requirements into these systems, their communications, or their interoperability layers. The result is that we have trillions of dollars of major weapon systems that are profoundly vulnerable to cyberattack. It is conceivable that the next major military conflict will be decided with the click of a mouse. Imagine the effect of a cyberattack against a satellite constellation, prepositioned defense stock, or a fleet of fighter aircraft positioned to respond to crisis. The cyberattack doesn't have to be dramatic to be devastating; the enemy just needs to ensure that those fighters cannot get off the ground to respond to an attack.

Today, the IT cybersecurity community aspires to concepts such as "zero trust," where all system interactions are suspect and should not be trusted. Unfortunately, major weapon systems are several decades behind. They are complete trust systems. Regrettably, we cannot redesign these systems with secure electronics and protocols because of the long timelines and astounding costs involved. All is not lost, however. We can draw strength from the tremendous progress that the cybersecurity community has made in securing IT systems. We do not need to reinvent the wheel. We can learn from thirty years of best practices to accelerate weapon system cybersecurity. Well known concepts like defense in depth, patch management, access controls, and incident planning are highly applicable to weapon system cybersecurity. This is far too big a job for one organization to solve. It will take a village—including government, academia, and industry—to get there. Each best practice reinforces the other.

In the world of major weapon systems where there is virtually no cybersecurity aside from obscurity, observability is the first step. Not only does it help you to design the other control measures, but it ensures that you are keeping up to date with the latest threats. To observe weapon systems—or any digital system for that matter—you need data collection. Weapon systems have data networks that connect all their electronic components. You can think of them like nervous systems. These nervous systems generate enormous amounts of extremely valuable data every second. Unfortunately, in 2018 no weapon systems collected all—or anywhere near all—of this data. These platforms were talking, but no one was listening.

Industry has tackled the weapon system cybersecurity observability problem by building the foundational tools first. The military now has readily available, certified hardware capable of real-time edge computing and software capable full-take data capture from every bus. Frameworks exist for normalizing, translating, and enriching the data into a common format. Technologies and processes for liberating this data from the weapon systems can be fed into cloud environments. This took years, but the military should be proud that it successfully completed its first full-fleet deployment last year and has already democratized many terabytes of critical data from that fleet. The services have begun many more initial deployments since.

Armed with this foundation widely deployed across the DOD—pristine, full, high-quality digital data streams from every weapon system—we would have the platform to build AI-enabled applications that can scale and integrate across platforms to support all domain operations. Intrusion prevention is a canonical example. In AI parlance, intrusion prevention is a "classification problem." Given a stream of data, you must detect anomalous/malicious traffic from normal/benign traffic. There

are several algorithms that are very good at detecting many kinds of cyberattacks against weapon systems. No need to reinvent the wheel.

But we're only able to unleash these algorithms once we build the data foundation.

We Are Out of Time

In very short order, we must aggressively expand this foundational work across our major weapon systems. There is remarkable work on enterprise architectures to promote ready, decentralized, self-service access to wide ranges of data, algorithms, and applications. We must expand the scope of these foundational efforts to include the trillions of dollars of major weapon systems that the warfighter relies on in both combat and training missions.

The extensive NSCAI report comprehensively addressed some very critical issues regarding the State of the AI ecosystem and produced an extensive series of key recommendations to change the paradigm of AI adoption. However, we do not have the luxury of time for drawn-out policy and budgetary cycles; if the U.S. does not take the lead on establishing and formalizing standards and responsible use of AI, our adversaries will.

Recent legislative activity highlights the congressional commitment to addressing the issue, but we must be mindful of the speed in which we consider the role of AI in defense. While our adversaries are developing and employing AI technologies at speed of requirement, we must be faster—we must consider how to deliver at the speed of action. As data continues to flow off weapon systems and associated sensors, the Department must consider the resource limitations it faces with sensemaking; there will never be enough DOD civilians or servicemembers to manage the biblical deluge of data—AI models must be employed to ensure a postured, ready, and resilient formation where the unnecessary risk of known vulnerabilities is addressed with smart models that can distinguish between anomalous alerts as maintenance issues or cyberattack.

While the Department defends their fiscal year 2024 budget requests, Congress must ask—are these budgets representative of change necessary to truly develop and posture a ready force? Does the Department consider readiness in terms of threats borne of the 21st century, or are they still articulating ability to fight through outdated, outmoded practices of failed history? Are the right steps being taken to buy down unnecessary risk based upon known vulnerabilities, or does emphasis remain upon those capabilities which might be useful today but useless tomorrow?

America's preeminence as a military superpower derives from several key inputs including the world's best trained and highest quality people, its robust budget, its global reach, and our tremendous allies and partners. But its technological superiority, especially manifested in our major weapon systems, is where we derive the greatest advantage. If, as the NSCAI's report warns, the United States doesn't retain its AI dominance and empower its major weapon systems with AI-enabled technology, we face the real prospect that an adversary could surpass us.

We must act now to prepare our major weapon systems for the era of AI. We are decades behind and there's not a moment to lose.

Senator MANCHIN. Thank you, sir. Now, we are going to start with our questions, and I will begin. I have been thinking about this because when you look at it, the internet was founded in, I think, 1983.

A Section 230 came into play in 1996, I believe. We have been discussing that ever since. Should we have done more? Should we have put—how are we going to put back the guardrails on it? Has it gone too far? Who is accountable? Who is responsible?

On and on and on. Now that we are coming into the age of the AI, give me your—each one of you, give me your thoughts on as this comes into the realm, if you will, and we are going to be so dependent on it and using it for so many purposes.

What could we do, learning from what we didn't do when the internet came into play? Dr. Matheny.

Dr. MATHENY. Thanks, Senator Manchin. I think that the application of some of these large models to developing very capable

cyber weapons, very capable biological weapons, disinformation campaigns at scale pose grave risks.

I think one of the threats that I see is that the very technology that we develop in the United States for benign use can be stolen and misused by others. I think we need a licensing regime, a governance system of guardrails around the models that are being built, the amount of compute that is being used for those models, the trained models that in some cases are now being open sourced so that they can be misused by others. I think we need to prevent that.

I think we are going to need a regulatory approach that allows the Government to say tools above a certain size with a certain level of capability can't be freely shared around the world, including to our competitors, and need to have certain guarantees of security before they are deployed.

Senator MANCHIN. You know, my biggest fear is that what little bit I know about AI, but knowing the capability of AI, having people say something they never said, having the image of a person doing something they never did, having a country declaring war that never happened.

All these things—I mean, the stakes are so high in what we are doing. But if we can learn from our mistakes and put those guardrails in now, and you all would know better of how you intend your program to be used or your platform to be used to tell us what shouldn't be there to protect not just this, to protect your market, if you will, that protect basically the use of this and the intentions of what it is for.

I think we need to do that and think about this deeply before we go further. Dr. Sankar—Mr. Sankar.

Mr. SANKAR. Absolutely. I think a lot of what you are getting at is we kind of implicitly all believe or explicitly believe that AI is valuable, but how do you make it viable? It is not viable without trust.

That trust requires a real foundation where you understand the data that went into it. You understand why, to the extent you are not getting behaviors you expected, you are getting those behaviors.

So, I think a big part of this approach is, you know, I would welcome a regulatory approach to this, is also realizing that there is a huge and outsized role for the Department to lead by going through it.

It is only by red teaming, adopting and red teaming trying to break it, that we are going to really understand and develop the appropriate rigorous testing and evaluation framework, I would say.

The analogy to cybersecurity is great here. You can't just have a blue team effort to protect yourself. You learn as much or more from red teaming it. That defines how you defend yourself going forward.

I think these are actually two sides of the same coin, and we should be practicing them together and aggressively.

Senator MANCHIN. Dr. Lospinosa.

Dr. LOSPINOSO. Thank you, Chairman. I totally agree, and I think that the analogy to the internet is really apt. If we have

learned anything in the past several decades of technology innovation, we see a focus on functionality first, in the case of the internet, sharing information—in the case of AI, solving a broad range of applications.

Then we think about security, and I think we can't make that mistake again. Today, we spend hundreds of billions of dollars on cybersecurity trying to shore up the problems that we had in the past that we didn't think about.

We have an opportunity now to think about the security of these AI models as well. There are two frontiers that I imagine we will probably get into later in the discussion. But to preview, you know, data poisoning is a huge problem.

So, the idea that the data you are using to train these models can be altered by nefarious actor to create profound challenges with the AI algorithms. The second is adversarial attacks. You may have seen some of these sensational videos of putting a few dots on a stop sign and to a self-driving car it looks like a green light.

Or fingerprint readers with a couple of modifications spoofing, you know, authentication. These are real problems, and we need to think clearly about shoring up those security vulnerabilities in our AI algorithms before we deploy these broadly and have to clean the mess up afterwards.

Senator MANCHIN. Well, let me just say thanks to all of you. Would it be possible I mean, I think on behalf of Senator Rounds, myself, and our Subcommittee here, to ask you all to as quickly as possible, 30, 60 days, put a little team together, give us some thoughts on what you think can be and should be done.

We can share them with the Committee Members here to see if we can launch, basically start looking at how we would write legislation not to repeat the mistakes of the past. If you could do that, we would appreciate it. Senator Rounds.

Senator ROUNDS. Thank you, Mr. Chairman, and look, I really want to thank our witnesses here today for some very good opening statements.

You actually answered a couple of questions that I had in advance just in the opening statements themselves with regard to the effects on National Security and our competitiveness. I want to get into something which is current in the news today, and that is there a group of fairly well-respected AI experts and industry leaders recently signed a letter calling for a pause in AI development, citing a risk to society.

I think the greater risk, and I am looking at this from an American, a U.S. security standpoint. I think the greater risk is taking a pause while our near-peer competitors leap ahead of us in this field. AI will be the determining factor in all future great power competition, and I don't believe that now is the time for the United States to take a break from developing our AI capabilities.

My questions to all of you would be, number 1, is it even possible to expect that other competitors around the world would consider taking a break? What could be the impact if we were to try to slow down our AI development while Congress looks at policy issues and the rest of the world continues on, in particular, our near-peer competitors who seem to have a considerably less announced concern with regard to the ethics of this new technology?

Dr. Matheny, I would like to start with you.

Dr. MATHENY. Thanks, Senator Rounds. I think it would be very difficult to broker an international agreement, to hit pause on AI development in a way that would actually be verifiable. I think that would be close to impossible.

I think we are taking appropriate first steps to create a governance system in which we could at least delay China's access, for example, to very high-performance computing thanks to the October 2022 export controls on AI chips and the subsequent controls on semiconductor manufacturing equipment.

But it is very difficult to say, internationally, we would be able to achieve some sort of pause in a way that is enforceable. It is also unclear how we would use that pause and whether we could use it effectively in a way that allows democracies to lead the norms and standards around AI and its implications for society.

I would like to see democracies maintain the lead. I do think an important part of maintaining the lead, though, is to ensure that we have guardrails. That we are seen as the beacon for safety and security considerations.

That will actually help to win as friends and allies around the world. Our democratic allies are looking to us for guidance, and I think we can be a first mover in some of the guardrails that are needed.

Senator ROUNDS. Thank you. Mr. Sankar.

Mr. SANKAR. Absolutely. I think the pause is—what is going to be different in 5 months and 29 days, we need to really think about that, other than ceding the advantage to the adversary.

I think the other part of it is, so there is the technological capability that we could become—every 2 days now, there is breakthroughs made that we didn't think was possible.

So, the pace is breakneck. We are talking about generations of advances. But I do think due to Dr. Matheny's point, actually, perhaps the bigger consequence is the nature of the AI. China has already said that these generative models must display socialist characteristics.

It must not enable the overthrow of the State. So, these sorts of constraints that are being baked into the extent that that becomes the standard AI for the world is highly problematic.

I would double down on the idea that a democratic AI is crucial. Now that is—we will continue to build these guardrails around this, but I think ceding our nascent advantage here may not be wise.

Senator ROUNDS. Dr. Lospinoso.

Dr. LOSPINOSO. Yes, sir. I totally agree. I think that it is impracticable to try to implement some kind of pause. I think if we did that, our adversaries would continue development and we end up ceding or abdicating leadership on ethics and norms on these matters if we are not continuing to develop.

That is not to mention the practical implications of us falling behind on, as Mr. Sankar mentioned, these applications that are incredibly important, cybersecurity, military applications.

We lose in that competition and we enfeeble industry that is working at breakneck speed to try to keep us on top.

Senator ROUNDS. I would just ask one, and I think this can be answered fairly quickly, and we will probably do a second round on it, but with regard to AI right now, isn't it true that there are literally dozens of countries around the world that have already implemented degrees of AI into their weapons systems that have already been deployed on the battlefield.

I am thinking of the Nagorno-Karabakh war between Armenia and Azerbaijan in September 2020, where loitering munitions were used that with no human in the loop, literally determined their own weapons—their own weapons to use on which objects without a human ever ordering it.

Dr. LOSPINOSO. Senator Rounds, that is exactly accurate. I mean, this is going to continue to develop. We are going to have autonomous weapons systems developed by other countries. If we are not continuing to invest in that research and development, and concurrently develop norms, ethics around the employment of those systems, we are going to abdicate our leadership position.

Senator ROUNDS. Mr. Sankar.

Mr. SANKAR. I concur with that.

Senator ROUNDS. Dr. Matheny.

Dr. MATHENY. Agreed.

Senator ROUNDS. Thank you. Thank you, Mr. Chairman.

Senator MANCHIN. Senator Schmitt.

Senator SCHMITT. Thank you, Mr. Chairman. Thank you all for being here and for your testimony, and willingness to answer questions on a very important topic that I think I don't speak for everybody, is sort of not knowing where all of this leads provides an opportunity, maybe even a bipartisan way to help shape some policy here.

AI and machine learning are at the forefront of technological innovation and the great powers competition between China and United States. It is critically important, and so your recommendations are important.

AI is a transformative tool, and like other tools that can move society forward, but is also ripe for abuse. We see this abuse already happening. China's implementation of AI has allowed for mass surveillance of innocent Chinese citizens who have no chance at privacy.

U.S. tech companies have a responsibility to ensure that these powerful tools don't fall in the hands of authoritarian regimes who use it for activities that run contrary to basic human rights.

I was deeply alarmed by Google and its departure from Project Maven on unfounded or concerns that they had that business with DOD was unethical. Yet continued AI research in China that could have very well contributed to the mass surveillance and repression of over 1.4 billion people.

We have to do everything we can to not only develop this technology, but also to ensure it is being done and used responsibly. I guess my first question here, and this is a long question, but I will go to you first, doctor.

In 2017, Google opened up the Google AI China Center, which focused on basic AI research in Beijing. While Google engaged in AI research under the watchful eye of the Chinese Communist Party, the company shunned the Department of Defense and broke

ties with DOD's Project Maven because of alleged ethical concerns. Ironically, shortly after Google opened up its AI China Center, Google erased its longtime motto of, don't be evil.

Why Google would coincidentally abandon this decades long motto while operating its AI research center in Beijing, I can't say for sure, but it doesn't look good. But I do know the Chinese Communist Party has engaged in basic human rights abuses, genocide, and mass surveillance of over 1.4 billion citizens.

Big tech companies like Google need to have the moral backbone to resist these grandiose ideas of market access and increased profits in exchange for IP [intellectual property] rights that could ultimately be used as an effective tool of repression in an authoritarian regime and also turned on us, the United States of America.

Despite Google closing its Beijing based AI Research center in 2021, the potential applications remain. General Dunford put it that any work by United States companies who aid China in the development of AI would, "help authoritarian government assert control over its own population," enable the Chinese military to take advantage of United States technology.

Dr. Lospinoso, do you agree with General Dunford's statement?

Dr. LOSPINOSO. Thank you for the question, Senator Schmitt. I wholeheartedly agree with General Dunford's statement. I think doing business in China is equivalent to providing technological capabilities to the Chinese military.

This is the great power competition of our time. I don't think it is a question of if, it is a question of when. Schiff5 has never and will not do business with the Chinese military, and we think it is a matter of utmost National Security.

Senator SCHMITT. Well, and I think—so, I am 47. So, when I was going to school and we were learning about these things, and I think for a long time, I think the belief was that you have a greater opportunity for democratization and the more educated people become they are aware of the opportunities, and that would ultimately be the way that the Chinese Communist Party would be overthrown from within.

The scary thing about AI is that AI only strengthens a communist regime's ability to control the flow of information. All of these assumptions that were made for a very long-time sort of go out the window.

AI in many ways is sort of built for an authoritarian regime, which I think in this great powers competition we are in not just with China, but around the world, it has implications that are, I think, really scary. So, I don't know, I mean, I think the American public is trying to figure this thing out, too.

For me, we have to engage from a military perspective because it is do or die quite literally, from a military perspective. But from a commercial application, it is really scary stuff. So just curious, I don't know how much time left, but for each of you, what keeps you up at night about this, and what can be done to address those concerns?

Dr. LOSPINOSO. I share those concerns, Senator. Briefly, the thing that keeps me up at night is, a fanatic here has been the central role of data, and the power of AI algorithms and their applica-

tions. I can think of few governments more adept at collecting and retaining data than the Chinese Communist Party.

The fact that they have such pervasive collection not only of their own citizens, but of citizens around the world through a variety of mechanisms. That gives them a significant leg up in using AI for the purposes that you articulated.

Mr. SANKAR. What keeps me up at night is, do we have the will? I think we do. But the issue of AI adoption is really one of will-power. Are we accelerating adoption like our survival depends on it, because I believe it does. I think you see that in our adversaries. They realize that their survival depends on it, and we should move at pace to do this.

Dr. MATHENY. What keeps me up at night is AI being applied to the development of new cyber weapons and bioweapons for which we don't have reliable defenses.

I worry that right now the most likely scenario is one in which those models were either stolen from the United States or built with U.S. tech, U.S. chips, U.S. chipmaking equipment.

I think the strongest argument for a pause is our own labs need to get their cybersecurity together to reduce the likelihood that the models that they are building will be stolen by our adversaries.

[Technical problems].

Senator MANCHIN. Dr. Matheny—thank you. Our hope today was to have witnesses from Scale AI present, because of scheduling they couldn't make it, to discuss their data management practices to ensure the data being fed into the algorithm is consumable. Just to put this in context for the public, private industry has to buy the majority of data they need to feed into their AIs.

But DOD is in a unique position, given the wealth of data we are collecting on a daily basis from every network, node, and physical sensors in all our equipment. The problem seems to be in owning that data and making sure it is all the same format for an AI to recognize and use.

My question is this, is it fair to say that the data an AI interprets and learns from is arguably more important than the algorithm itself?

Dr. MATHENY. I think it is all important. I mean, sometimes the analogy is used of, you know, three legs of a stool. You have got data, the algorithms, the compute, and then the floor is talent. I mean, that is something that is essential to all of those. So we need to invest in all four of those elements.

I do think that data can be a place where the United States has an asymmetric advantage because of the amount of data that we collect from systems that have operated globally in a way that, say, China's systems or Russia's systems haven't. This is an observation that the Director of Net Assessment at DOD made, which I think is accurate.

We simply collect more data from more platforms that are relevant to military operations than any other country. But we are not fully leveraging that. We need to ensure, one, that we appropriately collect, store, align the data, place it in data bases that can actually be leveraged.

I think one of the things that was most striking about Project Maven was just how much work had to be done on data cleaning,

alignment, getting networks to talk to each other. It was that stuff. It wasn't the sexy algorithm stuff that was the hard part. It was the elbow grease needed to just ensure the data was in the right place.

Senator MANCHIN. Any other comments from anybody else on the panel on that? I might have a followup to you. Here is a followup, so you can think about this, too. How would you summarize the Department of Defense's data management practices, and how could they be improved to make sure that every bit of data that we are collecting is available for our usage, not limited by silos between private contractors? That is kind of the followup to the first issue.

Mr. SANKAR. I would like to build on the stool analogy there, and I will get to your followup question. You can't make one leg of the stool long and tall first. That is not a very good stool.

I would urge us to resist the temptation to say, first we need the perfect data foundation, then we go on. Actually, it is, if we look at the Project Maven example, there is the fact that we suddenly had the algorithms that pointed us to the fact that the data was garbage. So, these things move together and we have to simultaneously coordinate the investment and not slice these up into different responsibilities.

It is now the fact that we have these powerful large language models that is telling us that we actually don't have enough CPU [central processing unit] capacity in the world, and so, you know, I think the stool analogy is a very good one.

Now to your question here, I would say this idea that we are operational is profound. It is our advantage. We do things everywhere in the world. I would say we definitely collect more data, but we also throw away an enormous amount.

Part of my experience has been every place we have shown up in a new operational context, there is data we could be collecting that in a prior generation of software was perceived to be useless because there was no operational decision you could have been making with that data so it was often thrown on the ground.

When new capabilities were introduced, the utility of that data became obvious on its face. So, this is a powerful feedback loop that really feeds into our American culture of innovation, solving problems at the edge with the capabilities we are providing. I would say the data management efforts are great.

There are definitely some policy opportunities that would make it world class. So how do we all get on the same page here? I think we have to get the incentive structure right around how we share data.

So, a mandate that all data must be shared because it is actually the Government's I think is great in theory, but in practice, in order to enable all of the folks with various interests to do that, you need a data foundation that gives you true security. How am I labeling this data? How do I control who has access to it?

How do I govern the purposes for which they are allowed to use this data? Once I develop trust in how we are governing access to this data platform within the Defense Department, now, we can actually share this data.

Senator MANCHIN. That was the question we are asking on the front end.

Dr. LOSPINOSO. Thank you, Chairman. I completely agree with everything that we said here. I would add, though, that while it is clear that we are the best in the world at collecting data, we have got some work to do on data architecture and access to that data.

I still want to emphasize that we have a significant amount of work to do with the computers that don't look like computers, these weapons systems that we operate around the world. I will tell you, when I was in uniform, it drove me absolutely crazy that we could operate an aircraft or a ground combat vehicle or a submarine in a combat environment and not, number 1, be able to collect or own the data that came off of that platform.

That is just a massive National Security issue. I think we need to get better at enabling these systems, these weapons systems with the kinds of data collection to feed into this data architecture so that we can get the enterprise IT [information technology] computer side as well as the weapon systems.

That is going to be our real advantage, and I will just end with one comment here, which is increasingly, you know, we had this conversation around cryptography when we were thinking about what can we put backdoors in the encryption.

There is a sense in which when these AI algorithms get out into the public domain, and there is academic papers and PhD thesis that are written about these things, they are kind of cat is out of the bag.

So, on some sense we should continue to try to keep models guarded, but that is a time advantage. At some point it is knowledge and it is going to get out there. The real advantage, what we can control is the data, that one leg of the stool that our adversaries won't have, and then we retain our leadership position and being able to employ these AI models.

Senator MANCHIN. Thank you all. We will continue this, but now, Senator Rounds.

Senator ROUNDS. Thank you. I want to followup with that. I am going to begin with Dr. Lospinoso. When we talk about data, China right now, the People's—the Chinese Communist Party has collected huge amounts of data on their own citizens.

We don't do that in the United States. But they have been very good about collecting it on their own people. We know that they have laid out not only facial ID, but they can track their people no matter where they are going, what they are doing, the transactions, their financial transactions, who they associate with and so forth.

They have been doing it for years, and they have gotten to be very, very good at it. They clearly are using AI. They have clearly figured out a way to do the types of data bases that can be manipulated to be able to go back and collect that data, we are assuming. In the United States—we need to be able to compete with that type of computing power and that type of data collection and storage.

Do we have that capability in like kind and quality, as China does today in terms of implementing it and using it? Do we have the practical application today that they have exercised in China on their own people?

Dr. LOSPINOSO. Thank you, Ranking Member Rounds. I would say that from a technological capability perspective, there is no reason that we couldn't implement the same sorts of platforms. Perhaps they have national foreign intelligence value, for example. Of course, we have ethics and freedom constraints that keep us from doing the same sort—

Senator ROUNDS. Which we absolutely have to protect.

Dr. LOSPINOSO. Absolutely have to protect—

Senator ROUNDS. We have to protect privacy in the United States.

Dr. LOSPINOSO. I would say that one opportunity here potentially is we talked about ways in which AI algorithms can be subverted. I think there is an opportunity for us to also make investments not only on the defensive side, but on the offensive side when we are talking about great power competitions in thinking about how do we subvert adversary AI as well.

There is an asymmetry to these sorts of things that is corollary to cybersecurity, where sometimes the best defense is a good offense.

So I think we ought to be investigating ways in which adversarial AI and things of that nature, data poisoning might be able to meaningfully degrade the just objectively terrifying developments that we are seeing in some of these things, like the social scoring and, yes, the over the intelligence apparatus that the Chinese Communist Party—

Senator ROUNDS. Thank you. Dr. Matheny, you were involved in the AI Commission, specifically with regard to defense. I have had the opportunity to see not just the unclassified but the classified report.

Recognizing that we are in an unclassified environment here, I would simply express that I think there was a huge amount of extremely valuable data that was found in the classified portion that transcended the Defense Department's needs and really went into areas that could be extremely helpful to other parts of our governance system.

Clearly, in terms of health care, truly making a quality difference in a lot of people's lives long term, if we could appropriately use and promote AI in a number of different fields. Can you talk a little bit—let me just express my frustration.

It was so classified that in many cases chairmen of other committees that could have utilized the data or the ideas that were recommended, that they didn't even have access to the reports or the recommendations.

I found that to be extremely concerning. I would just like you to share a little bit, if you could, how much of an opportunity the implementation, the appropriate implementation of AI could mean to the quality of life to people that live in this country?

Dr. MATHENY. Thanks so much. I will take it back to our fellow commissioners and to the NSCAI staff the opportunity to think about how to create a tearlined version of the classified annex at a lower level of classification. I do think that the opportunities to solve society's problems with AI are profound.

The applications to advancing human medicine, energy, agriculture, and materials science. We are seeing some early signs of

that, everything from Alpha fold, solving the protein folding problem to make protein design possible at scale for new drugs, or the design of new fusion reactors, or solving math problems that had eluded human ingenuity for years.

So, the positive applications are so profound that we have to figure out a way to put appropriate guardrails so that we get the upside without the downside.

Senator ROUNDS. Thank you. Dr. Sankar, would you like to add anything with regards to the opportunities that AI provides to this country if we properly implement its use?

Mr. SANKAR. I think the opportunities are world changing.

The way for us to maximize that is to align behind them. You know, we have significant growth in our health care costs. How do we align behind the application of AI to driving the national outcome that drives patient care and quality?

So, I think there are a couple of places where Government leadership, where the issue is not capital, its customers.

Providing the sort of bootstrapping foundational customer to drive the concentration of energy to solve the problem and to realize where we need policy to help us reorganize the many seams that are between here and realizing the benefit for American citizens.

Senator ROUNDS. Thank you. Thank you, Mr. Chairman.

Senator MANCHIN. Senator Schmitt.

Senator SCHMITT. Thank you, Mr. Chairman. Dr. Matheny, you just mentioned something that struck me as getting the upside without the downside. Is that really possible, though? Like the concern that I get it—but it seems to me that we have got a tiger by the tail. There is not going to be a pause.

It is moving. The choice that we have is, are we going to lead or not lead, right? From a military perspective, the answer is very clear, we have to. But getting back to the initial question, what role does the Government have by way of regulation that can—what would you suggest?

Not—and I throw this for all three of you, because there is a downside and the downside—we will feel the downside. But I guess from a risk mitigation perspective, what can be done because, you know, I am a lawyer. A very popular profession, but, there is going to be—right, well-being.

Yes, combine those two, Mr. Chairman. But, a lot of the, what first your associates did 10 years ago, that is gone. There is displacement that you are going to see everywhere.

But what would you guys suggest as far as—so that we minimize some of the risk that—the bad things that can happen?

Dr. MATHENY. I think there are good—

Senator SCHMITT. I don't mean displacing lawyers. That is not one—

[Laughter.]

Dr. MATHENY. That is right. No, that is off the table. Absolutely. I do think there are good pre-regulatory and regulatory steps that the Department of Defense can help to lead in.

The first is thinking about using Defense Production Act authorities to require that companies report when they are training very large models, how they are training very large models, where those

models are going, and preventing open sourcing of models that could be used by adversaries maliciously.

Also including in DOD contracts, cloud computing provider requirements that they know their customers before they provide services, not just for the DOD customer, but for all customers. This is really an extension of the common rule that is already a feature of Federal contracts for other purposes.

So, this already has precedent and use. The same for AI developers to know their customer and to develop cybersecurity requirements in our contracts so that those developers are less likely to get their models stolen.

Mr. SANKAR. I might add on to that too. There might be two aspects to the tiger's bite here. The first is, as you think about regulation, one of the realities of these AI models is that they are actually brittle.

That is the failure condition. That in the sweet spot, they seem magical. They seem more than human like, and just even one iota outside of the sweet spot, they become moronic. If you are trusting a moron, that is a problem.

So then how—the regulation framework is really about understanding the surface area and red teaming the model—where is the model going to work? Where is the behavior unexpected?

What do I expect of the model makers in terms of continuously testing as they upgrade and develop the model so that it is behaving in accordance to what the model is supposed to do? Those expectations are going to be different in health care than they are going to be in defense.

I think that is a generalized way of thinking about where is the risk in a concentrated basis. The second aspect of the tiger's bite is what it means for American prosperity. Technology is supposed to drive increases in productivity. The kind of basic economic theory here is those increases in productivity lead to increases in our standard of living and wages.

Hold tech companies accountable to that. Where are the increases in wages? If I am deploying this technology to a manufacturing company, the workers should be better off, not displaced. It is actually a choice, and I would say an abandonment of our obligation to the Nation to simply say, I have no opinion on how the technology is deployed.

Of course, AI is going to replace workers. That is not a foregone conclusion. AI can make those workers more valuable, it can drive up their productivity, and they should capture the growth of wages as a result. Concomitantly, with the company capturing value in the market from doing so. I think tech companies need to do more here.

Dr. LOSPINOSO. I would concur with all of that. I would say there is a need for regulation, unfortunately, because there—it is really hard to put technical controls in place that are going to prevent folks from doing the sorts of things that Dr. Matheny is concerned about. I also think that the displacement of workers compensation is really important as well when we talk about policy.

I mean, we have been for over 100 years talking about creative destruction, right. You learn about this in basic economics, Joseph Schumpeter. There are technological innovations that create dis-

placements and folks are sort of temporarily out of work. We retrain them and then raw economic output is stronger than ever before because we figure out ways of using the new technology.

I think we need to be thinking about ways of training and empowering folks that will be disrupted by technology. But ultimately, they are going to be faster, more efficient.

We are going to elevate those workers out of routine, mundane, error prone tasks into more advanced kinds of modes of work needed. From a policy perspective, think about how we ease that transition from where we are today onto where we are going tomorrow.

Senator SCHMITT. Thank you.

Senator ROUNDS. On behalf of the Chairman, Senator Peters.

Senator MANCHIN. I am so sorry. I am going to have to leave. You are in much better hands with Senator Rounds here. I want to thank you all. It has been great. I just want to say this, that I think that as the world turns, if you will, and what is happening around the world and all of the different buildup military might.

Just got back from Poland and Ukraine, saw what was going on there. I want to talk to you a little bit more about Maven and we will get into that later. My concern truly is this, this is a game changer. They can be developing all the super hypersonic missiles and everything else and all that space and everything else, this changes the game, whether they can deploy it or not.

If we are able to have that information and be able to source that to a point where we have more input and be able to be more accurate in what we are deploying, I think it changes the game for the United States to continue to be the superpower of the world. So, I want to thank you all, and we really need your input and help and look forward for your recommendations.

Senator Peters, before you came, we talked about what had happened with the internet came in 1983, section 230 came in 1996. We made so many mistakes. We are trying to really go back and we are having a hard time. We want to prevent that from happening.

They are going to give us—we asked them to give this Committee the recommendations on what we could do to put the guardrails in place that we can be superior in this and make sure that their product or their platforms aren't misused for nefarious situations.

Senator PETERS. Thank you, Mr. Chairman, Ranking Member. I just, coming in your conversation on the disruption for employment and what that is going to mean going forward. You are right, I am not like a robot apocalypse guy or anything, thinking that all of our jobs are going to disappear and the robots are going to be in charge.

But we know when you talk about disruption, my sense is this is more disruptive than anything we have seen. Some people compare this to like the printing press and the steam engine, things of that nature, which were big.

As I think about this, what was different that time is it took a lot of time for that technology to actually get through the system. When you are talking about the industrial revolution, is probably over 150 years, and we are all benefiting from the industrial revolution of 150 years. But in 150 years we had world wars, the rise of communism and fascism, and political discord.

This may happen in less than a decade versus 150 years. So, the speed of this—has us all very concerned. I am glad you are thinking about this, but we have got to try to stay ahead. I don't know how you can stay ahead because of the rapid pace of what this is going, which is why we are going to need your help going forward.

As the Chairman mentioned, we want to make sure that the United States continues to be at the forefront. But, part of that are—really are the investments. So, I would just be curious, as from a Government perspective right now, what should be our priorities in investing to make sure that we are able to use AI with enhancing our ability to secure our networks and cybersecurity.

Maybe each of you kind of give me your, what do you think is one or two priorities for investments that we are not making now, or maybe we are, we should do more, or ones that we should be considering that we are not doing now? Whoever wants to start.

Mr. SANKAR. Senator, I will start. I will take a stab at it. I think the key thing is we should be using AI, right. So, there is a lot of focus on the models, the foundational capabilities, the infrastructure, developing the AI.

But AI is not a standalone capability. It has to be brought to bear in the application. I think one of the real experiences for Maven and certainly in the commercial world is you can't really bolt this on exposed to existing infrastructure.

You will find that that is limiting you and it forces you to re-imagine the user interfaces, the software approaches, the actual pane of glass you are using to make decisions. So, I think the long pull in the tent for us, where we are in this AI cycle is getting busy using it.

I think that also informs policymakers on the risks, both on the adversarial sense, but perhaps more importantly, the risks to jobs and how we are going to manage our way through that.

Senator PETERS. Great. Thank you.

Dr. LOSPINOSO. Thank you, Senator. I think the single biggest asymmetric threat that we face today is, in a world of near peer conflict, is the cybersecurity of our weapons systems. You know, I spoke in my opening remarks about the GAO's [Government Accountability Office] 2018 cybersecurity weapons systems report, unclassified.

You can sort of read about these broad problems that exist across basically every major weapon system we have. We have made disconcertingly little progress. In talking to program managers, it is a funding and requirements problem on these legacy weapons systems.

We are making great progress on new weapons systems and thinking about how do we encode requirements in these platforms to make sure that this aircraft is going to take off when we need to gain air superiority over an area.

I think that enabling those program managers to make the investments in building cybersecurity into these platforms is of the utmost importance. I will also just make a side comment here that many of these investments come together and are mutually supporting.

So, one of the ways that we bring cybersecurity to our weapon systems, to our enterprise networks, is through observability, and

observability is rooted in data. By collecting data off of these weapon systems, we are also supporting things like AI ready and AI enabled military.

We are currently not collecting the vast majority of data that these weapon systems are collecting, so I would highly recommend that that is a very high ROI [return on investments] area for investment.

Senator PETERS. Before we go to the next, so collecting the data, which is the key thing, especially when we are looking at automation—I am really involved with self-driving cars on the commercial side from—in Michigan, but it is all about having a massive dataset.

We have all of these weapon systems out there that are collecting it, but you are saying it is not collected in one place, it is not really usable to train our systems. That should be a priority.

Dr. LOSPINOSO. Yes, Senator. So, the actually the vast majority of data that these systems generate evaporates into the ether without ever getting collected, unfortunately.

We struggle mightily with extracting even the simplest data streams off of the vast majority of our major weapons systems. In some cases, that is just because we haven't made the investment.

In other cases, it is because the defense primes, frankly, lock that data up and they don't want the Government to have access to it because they want to use that as an opportunity to build additional products or services on top of that platform.

I think that if we are going to win in a near-peer conflict, the DOD needs to own the data that its weapon systems are generating in a combat environment. I think that we really need to pay attention to that.

Senator PETERS. Yes, I would like to pursue that further with you at some point.

Dr. MATHENY. I think given the massive private sector investment in AI right now, it makes sense for the Federal Government to concentrate on the places where it has a unique role, where there is a market failure or an authority that only the Government can exercise.

One of those, I think among the most important, is in thinking about the talent that is needed to support AI development in the United States. One of our leading sources of talent is global, and the United States has an amazing asymmetric ability to attract scientists, engineers from around the world, but we often don't let them stay.

We are punishing ourselves by not taking advantage of this asymmetric capability that the United States has to serve as a magnet for global talent. So, I think that is essential. If we want to win that competition against a country that is four and a half times our size, is producing more PhDs than we are, twice as many master's students in STEM [science, technology, engineering, and mathematics] fields, we have to attract the global team to join ours.

A second key area is cybersecurity requirements for the leading AI labs so that they are less likely to have their models stolen. A third is export controls on chips and chip making equipment so that our competitors don't have access to leading edge compute.

A fourth is Federal research that is focused on the places where the commercial sector is going to under invest, including in AI security and safety, but also thinking about how we break other countries' models, because I think these models right now are very brittle.

We need to be thinking about ways that we can slow down progress elsewhere by doing things like adversarial attacks, data poisoning, model inversion. Let's use the tricks that we are seeing used against us and make sure that we understand the state-of-the-art.

Senator PETERS. Best defense is a good offense, is that your point? All right. Thank you. Thank you, Mr. Chairman.

Senator ROUNDS. Thank you, Senator. We are getting close to the end of the session, I think. I am not sure if any other Members that are coming in, but I just want to recognize, and Dr. Matheny, I think you hit it on the head with regard to our need and the discussion about a legal immigration system that allows us to bring in talent that benefits our country.

Can you imagine a world today if Albert Einstein had not been allowed into our country? The world would be a different place today and not to the betterment.

I want to thank you all and I want to end with one that I sometimes think that when we have an unclassified session like this, we don't get an opportunity to get into some of the deeper items, but we also sometimes miss the opportunity to perhaps explore a little bit about some of the basics that just in terms of trying to explain what AI is.

I would like to offer a scenario, and then briefly, I would like to have you be critical of my analysis, if you would, please, Okay. So, looking at this, because I am a pilot and I think about what we have right now with regard to computing capabilities in most of the aircraft today.

We have an autopilot which once a pilot has departed a runway, they basically can set the heading, turn the autopilot on, set the heading, tell it to navigate to a particular point that they have already programmed in, set the altitude, and then lay in an arrival and an approach. That autopilot, will, with very few exceptions and with no more touching by the human, fly that course.

If there is changes along the way, frequencies and so forth in terms of communication, the pilot will make those modifications, so that the monitoring is constantly going on. With AI, it would appear to me that we are not really talking about an autopilot approach anymore.

What we are really talking about is having a system that does everything that the human does, but in a much more orderly and defined and disciplined way, so that it not only does everything that an autopilot would do, but it also makes the decisions about how to get there in the first place and where it wants to go.

Now having me said that, can you criticize or be critical of my analysis so that folks back home get a better sense of what AI means as opposed to simply talking about very powerful computers? Mr. Sankar, I hope that you have had an opportunity to go first. Let me put you on the spot first, sir.

Mr. SANKAR. Well, I think at the limit your vision is right, but I think you have to earn your way there. If we think about how long it took us with self-driving cars. I think the folks who have done really well, they are shipped incrementally. It is like we made the car a little bit more autonomous every single day.

At this point it is quite compelling. There is still, you know, can't do the snow, can't do certain low visibility conditions, but they are going to earn their way there. So, as we think about what is this likely to be today, I think these are tools, not agents. They can become agents. That is kind of the journey we are on.

But we are not going to get that for free. That is a lot of hard work that we are going to collectively do between here and there. I think for a lot of things today, the AI is a median human, which means it is going to be great at replacing a lot of tasks that allow our humans to do things that are cognitively more interesting.

The brittleness of the AI means that for new creative things, there is likely going to be an editor role. It is going to take our humans from being doers to managers, and that gives them a huge amount of leverage. In the same way that technology for all of history has given us a huge amount of leverage.

We sometimes underestimate what it has meant for us to have a palm sized supercomputer in our pocket. But profound, and I think we will look back and say the changes were just as profound, but perhaps slightly different than we anticipated.

Senator ROUNDS. Thank you. Dr. Lospinoso.

Dr. LOSPINOSO. Thank you, sir. I think we are in a really exciting era and things like ChatGPT have really enraptured people because we were talking about this before the testimonies, there is a level we have crossed with these generative AIs that it is surprisingly good.

Oftentimes if you just start a draft of something or you are iterating on some initial ideas, whether it is for, it can write poetry, it can generate images, it is displaying what we would start to think of as some form of intelligence. I think that is, sir, what you are kind of getting at, is we are past the point of, is this a water bottle or a cup of coffee?

Now we are talking about what would be interesting flavors to put in the water bottle. It is a gray kind of fuzzy line, but I share the sentiment that we are entering into a new territory with these models where we are not just doing the classic clustering, classification, prediction types of things.

We are starting to get into territories that were up until very recently reserved for human brains. We have got a lot of work to do, and I think we need human oversight of these mechanisms.

But even in our own personal experience, I think they have been really powerful at initial drafts of papers and things of that nature. So, we are going to see a lot of progress.

Hopefully the planes aren't fully flying themselves, there is still a human being in them for some considerable time, just given what we know about the brittleness of these models, so.

Senator ROUNDS. Thank you, sir. Dr. Matheny, last word.

Dr. MATHENY. I think we have got co-pilots in training. It still requires a lot of human supervision. But while they are getting

more capable, we need to develop the licensing regime so that they get a pilot's license at the end that we can be confident in.

Senator ROUNDS. Yes. Thank you. Thank you to all of our witnesses for coming and sharing with us today. This—on behalf of the Chairman of the Subcommittee, we will now adjourn. Thank you.

[Whereupon, at 10:48 a.m., the Committee adjourned.]

