Stenographic Transcript
Before the

Subcommittee on Cybersecurity

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON
THE STATE OF ARTIFICIAL INTELLIGENCE AND
MACHINE LEARNING APPLICATIONS TO
IMPROVE DEPARTMENT OF DEFENSE OPERATIONS

Wednesday, April 19, 2023

Washington, D.C.

ALDERSON COURT REPORTING
1111 14TH STREET NW
SUITE 1050
WASHINGTON, D.C. 20005
(202) 289-2260
www.aldersonreporting.com

HEARING TO RECEIVE TESTIMONY ON THE STATE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING APPLICATIONS TO IMPROVE DEPARTMENT OF DEFENSE OPERATIONS

Wednesday, April 19, 2023

U.S. Senate
Subcommittee on
Cybersecurity,
Committee on Armed Services,
Washington, D.C.

The subcommittee met, pursuant to notice, at 9:32 a.m., in Room 222, Russell Senate Office Building, Hon. Joe Manchin, chairman of the subcommittee, presiding.

Subcommittee Members Present: Senators Manchin [presiding], Peters, Rosen, Rounds, and Schmitt.

OPENING STATEMENT OF HON. JOE MANCHIN, U.S. SENATOR FROM WEST VIRGINIA

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 of RAND Corporation and Commissioner of the National Security Commission on Artificial Intelligence. 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 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 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 meaning -- 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?

Lastly, 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 NDAAs. 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.

But there too, we still have progress. We can make -- 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 HON. MIKE ROUNDS, U.S. SENATOR FROM SOUTH DAKOTA

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.

And 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 five 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. And 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 nonprofit, 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. And 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.

And 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.

And 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.

And 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. Matheny follows:]

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. And in that future, AI rewrites our roadmaps. It changes everything. And we can either choose to accept that disruption and drive that change, or we can get disrupted by defending against it. And because the future is already here, we need to act with speed and conviction. And 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 eye 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.

And 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 and AIG 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 60s, 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. Sankar follows:]

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 begun to capture the public imagination. I commend the subcommittee for treating this accelerating development with renewed urgency.

In 2021, the National Security Commission on Artificial Intelligence message was clear, if trends continue, China will surpass us within a decade. This subcommittee has asked whether we have made progress towards 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 one, most major weapons systems are not AI ready. As data scientists are quick to say, garbage in makes garbage out.

And 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 two, the DOD cannot solve weapons systems cybersecurity without artificial intelligence. Without AI, the DOD will never be able to keep these weapon systems

cyber secured. 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:]

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

A Section 230 came into play in 1996, I believe. And 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.

And 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.

And 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.

And 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.

And 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.

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

Senator Manchin: Dr. Lospinoso.

Dr. Lospinoso: Thank you, Chairman. I totally agree. And I think that the analogy to the internet is really apt. You know, 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.

And 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. And 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. And the second is adversarial attacks. So, 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.

And 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 one, is it even possible to expect that other competitors around the world would consider taking a break? And 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?

And 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 of '22 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 five 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 two 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.

And 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.

And that is not to mention the practical implications of us falling behind on, you know, as Mr. Sankar mentioned, you know, 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: And 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 of 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. And 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.

But 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 the activities -- 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, you know, 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 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. And so General Dunford put it that any work by U.S. 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 U.S. 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. Schift5 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.

And so, 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 -- 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 applications. And I can think of few governments more adept at collecting and retaining data than the Chinese Communist Party.

And 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? And I think we do. But the issue of AI adoption is really one of willpower. You know, are we accelerating adoption like our survival depends on it, because I believe it does. And 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.

And 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. And we need to ensure, one, that we appropriately collect, store, align the data, place it in databases 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 follow up to you. Here is a follow up, 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 follow up to the first issue.

Mr. Sankar: I would like to build on the stool analogy there, and I will get to your follow up question. You have to -- you know, you can't make one leg of the stool long and tall first. That is not a very good stool.

And so, 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.

And 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 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. And 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. And 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 governance 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 one, be able to collect or own the data that came off of that platform.

That is just a massive National Security issue. And 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 computer side as well as the weapon systems.

And that is going to be our real advantage. And I will just, you know, 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.

And 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.

And 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 follow up 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.

And 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 databases 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? Is 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. And perhaps they have, you know, national foreign intelligence value, for example. Of course, we have, you know, 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, you know, one opportunity here potentially is, you know, we talked about ways in which AI algorithms can be subverted. And I think there is an opportunity for us to also make investments not only on the defensive side, but on the, you know, offensive side when we are talking about great power competitions in thinking about how do we subvert adversary AI as well.

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

And so I think we ought to be investigating ways in which adversarial, you know, 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, you know, the social scoring and, you know, 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.

And 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.

And 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. And 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. And 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.

And 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.

This is -- it is moving. So, the choice that we have is, are we going to lead or not lead, right? And 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, you know, there is going to be -- right, well-being.

Yes, combine those two, Mr. Chairman. But, you know, a lot of the, what first your associates did ten years ago, that is gone. You know, and 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: And 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. And 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. And so, 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.

But 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. And 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, you know, concerned about. And 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. I mean, this is you learn about this in basic economics, Joseph Schumpeter. There are technological innovations that create displacements 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, you know, routine, mundane, error prone tasks into more, you know, 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. And you are in much better hands with Senator Rounds here. And, but 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 build up 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 after -- 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.

And 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 -- you know, 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. And 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.

But 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. But 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.

And as the chairman mentioned, we want to make sure that the United States continues to be at the forefront. But, you know, part of that are -- really are the investments. So, I would just be curious, as from a Government perspective right now, you know, what should we be -- 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 reimagine the user interfaces, the software approaches, the actual pane of glass you are using to make decisions. And so, I think the long pull in the tent for us, where we are in this AI cycle is getting busy using it.

And 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 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. And 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.

And I think that enabling those program managers to make the investments in building cybersecurity into these platforms is of the utmost importance. And 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 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.

And 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, you know, use that as an opportunity to build additional

products or services on top of that platform.

And 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. And 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 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.

And 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 programed in, set the altitude, and then lay in an arrival and an approach. And 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.

And 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. And 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.

And 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, you know, it can generate images, it is displaying what we would start to think of as some form of intelligence. And I think that is, you know, sir, what you are kind of getting at, is we are past the point of, you know, is this a water bottle or a cup of coffee?

Now we are talking about, you know, what would be interesting flavors to put in the water bottle. And 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. And we have got a lot of work to do, and I think we need human oversight of these mechanisms.

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

And, you know, 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 hearing was adjourned.]