[H.A.S.C. No. 118–37]

MAN AND MACHINE: ARTIFICIAL INTELLIGENCE ON THE BATTLEFIELD

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

HEARING HELD
JULY 18, 2023

U.S. GOVERNMENT PUBLISHING OFFICE
53–627 WASHINGTON : 2024

SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

MIKE GALLAGHER, Wisconsin, *Chairman*

MATT GAETZ, Florida
LISA C. MCCLAIN, Michigan
PAT FALLON, Texas
DALE W. STRONG, Alabama
MORGAN LUTTRELL, Texas
JENNIFER A. KIGGANS, Virginia
NICK LALOTA, New York
RICHARD MCCORMICK, Georgia
RO KHANNA, California
SETH MOULTON, Massachusetts
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
ELISSA SLOTKIN, Michigan
JARED F. GOLDEN, Maine
PATRICK RYAN, New York
CHRISTOPHER R. DELUZIO, Pennsylvania

SARAH MOXLEY, *Professional Staff Member*
MICHAEL HERMANN, *Professional Staff Member*
BROOKE ALRED, *Research Assistant*

CONTENTS

MAN AND MACHINE: ARTIFICIAL INTELLIGENCE ON THE BATTLEFIELD

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION,
Washington, DC, Tuesday, July 18, 2023.

The subcommittee met, pursuant to call, at 9:00 a.m., in room 2118, Rayburn House Office Building, Hon. Mike Gallagher (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. MIKE GALLAGHER, A REPRESENTATIVE FROM WISCONSIN, CHAIRMAN, SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

Mr. GALLAGHER. The subcommittee will come to order.

I ask for unanimous general consent that the Chair be authorized to declare a recess at any time. Without objection, so ordered.

I want to briefly review the three commandments of the CITI [Cyber, Information Technologies, and Innovation] Subcommittee.

One is that we shall start on time, which we just did. So that is good.

We are going to enforce the 5-minute rule, but if time allows, we will entertain a second round of questions, and it often does.

But I bring this up, I want to stress the third commandment, which is "Thou shalt not use acronyms or jargon," which I think is particularly important in this discussion because discussions about AI [artificial intelligence] can quickly degenerate into jargon-laden discussions.

We have three true experts on this topic, but just don't assume your average Member of Congress—or let me just say, don't assume I understand what you are talking about when you get into the nuances of AI. So we want to have a discussion in the open that your average American can understand today. We are asking you to demystify a lot of the concepts surrounding AI.

And in thinking about this topic that may sound counterintuitive, but I have been going back to the history of the early Cold War. In particular, I'm obsessed with the Korean war, which is the moment in which the Cold War first turned very hot, and at great cost to Americans, at even greater cost to the Korean people themselves.

And I was reading this sort of obscure book about it and came across the words of a historian named David Rees, who said, "At the heart of West military thought lies the belief that machines must be used to save its men's lives. Korea would progressively be-

come a horrific illustration of the effects of a limited war where one side possessed the firepower and the other the manpower."

There's a lot of different ways to interpret this in the current context, and particularly in the context of this hearing.

One is that AI could potentially increase the destructive power of modern warfare.

The other is AI has the potential to decrease it, or at least decrease the exposure that our soldiers, sailors, airmen, and Marines take when they put themselves in a combat situation.

Or the third—and what is unique, in contrast to the early Cold War—is that the machines themselves might somehow take power and go beyond our ability to control them.

Today, we want to dig into all of these different hypotheses. The only thing, as I have dug into this topic, and I want to commend the ranking member, Mr. Khanna, for the way in which he has worked with me to really use the subcommittee to explore AI concepts.

We had a very fascinating discussion with Elon Musk last week. I will say there were some sources of disagreement. Mr. Musk believes China is on "Team Humanity." I'm not persuaded of that point. And the only thing I have become convinced is that the CCP [Chinese Communist Party], if they win this competition or win the sort of AI component of this competition, will likely use that technology for evil, as a way of perfecting a oppressive totalitarian surveillance state, as well as exporting that model around the world. Whereas, we in the West, we in the free world at least have the chance of using it for good.

So to make sense of all these things, we are lucky to have three incredible witnesses.

Mr. Alex Wang is the CEO [chief executive officer] of Scale AI. And I don't know, you might be the most successful MIT [Massachusetts Institute of Technology] dropout of all time at this point, but there's actually probably a unique subset of people that qualify there.

Mr. Klon Kitchen is senior fellow at the American Enterprise Institute and someone many of us on Capitol Hill look for for advice when talking about the intersection of technology and warfare.

And Dr. Haniyeh Mahmoudian of DataRobot is an absolute AI expert as well.

So I have been looking forward to this hearing for a long time. I look forward to an open and honest discussion. Just remember, no acronyms, no jargon.

And with that, I yield to the ranking member, Mr. Khanna.

STATEMENT OF HON. RO KHANNA, A REPRESENTATIVE FROM CALIFORNIA, RANKING MEMBER, SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

Mr. KHANNA. Thank you, Mr. Chairman, and thank you for convening this panel and your interest in a bipartisan way in addressing AI and making sure that our military is leading with AI. I have appreciated how you have approached this throughout your chairmanship.

I'm not going to be long because I know people want to hear from the witnesses. I would just say that my understanding is that

China is spending almost 10 times as much as the U.S. as a percent of their military budget on AI, and we really need to think about the modern technologies that are going to be needed to have a most effective national security strategy.

So I'm particularly curious from the witnesses about how they think America can maintain and have the lead in AI technology going forward, what are the investments we need to make, and what are the standards we need to have to ensure that our AI is used most effectively. I'm looking forward to this panel.

Mr. GALLAGHER. Thank you.

Mr. Wang, you are now recognized for 5 minutes.

STATEMENT OF ALEXANDR WANG, CHIEF EXECUTIVE OFFICER, SCALE AI

Mr. WANG. Chairman Gallagher, Ranking Member Khanna, and members of the subcommittee, my name is Alexandr Wang and I'm the founder and CEO of Scale AI.

It is an honor to be here today to testify at the dawn of this new era of warfare—one that will be dominated by AI—and what the United States must do to win.

In 2016, I founded Scale with a mission to accelerate the development of AI. From our earliest days of working with the leading autonomous vehicle programs at General Motors and Toyota; technology companies such as Meta, Microsoft, and Open AI; and partnerships with the U.S. Government, including the U.S. Department of Defense's CDAO [Chief Digital and Artificial Intelligence Office], the U.S. Army, and the U.S. Air Force, we have been at the forefront of AI development for more than 7 years.

The country that is able to most rapidly and effectively integrate new technology into warfighting wins. If we don't win on AI, we risk ceding global influence, technological leadership, and democracy to strategic adversaries like China.

The national security mission is deeply personal for me. I grew up in the shadow of the Los Alamos National Lab. My parents were physicists and worked on the technology that defined the last era of warfare, the atomic bomb.

The Chinese Communist Party deeply understands the potential for AI to disrupt warfare and is investing heavily to capitalize on the opportunity. I saw this firsthand 4 years ago when I went on an investor trip to China that was both enlightening and unsettling.

China was making rapid progress developing AI technologies like facial recognition and computer vision and using these for domestic surveillance and repression. That same year, President Xi Jinping said, quote, "We must ensure that our country marches in the front ranks where it comes to theoretical research in this important area of AI and occupy the high ground in critical and AI core technologies." End quote.

China is investing the full power of its industrial base for AI. This year, they are on track to spend roughly three times the U.S. Government on AI. The PLA [People's Liberation Army] is also heavily investing in AI-enabled autonomous drone swarms, adaptive radar systems, autonomous vehicles, and China has launched

over 79 large-language models since 2020. AI is China's Apollo Project.

To lead the world in the development of AI, we must lead the world in the amount of high-quality data powering AI. Scale is firmly committed to doing our part to support the U.S. Government and ensure America maintains its strategic advantage. Today, we do so in three ways.

One, Scale data engine. We annotate and prepare vast troves of data for the U.S. Government.

Two, autonomous mission systems. We partnered with DIU [Defense Innovation Unit] to develop a data engine that will support the Army's Robotic Combat Vehicle program.

Three, we developed Scale Donovan, our AI-powered decision-making platform that rapidly helps the U.S. Government make sense of real-world information.

The DOD [Department of Defense] has also taken a number of steps in the right direction, most notably with the launch of the Chief Digital and Artificial Intelligence Office.

While this progress is promising, more must be done to achieve AI overmatch. AI Overmatch is our five-pillar plan to maintain the United States' security and technological edge in this new era.

First, investment in AI. It is critical to increase America's investment to maintain our leadership. Despite record AI investment in the fiscal year 2024 President's budget, the U.S. is still spending three times less than China.

Second, data supremacy. AI systems are only as good as the data they are trained on. The DOD creates more than 22 terabytes of data daily, most of which is wasted. AI warfare requires leading the world in developing AI-ready data.

Scale fully supports the CDAO and its legislative mandate to establish a centralized data repository, which would enable the DOD to harness the power of data with AI.

Third, testing and evaluation. It is one of the most important ways to ensure that AI models are accurate, reliable, and uphold the DOD's ethical AI principles.

The administration has embraced this concept by highlighting Scale's role building an evaluation platform for frontier LLMs [large language models] at DEFCON [hacker conference].

Fourth, pathfinder projects. Congress should authorize and fund new programs with the mission of developing innovative AI-powered warfighting capabilities. Since Project Maven was started more than 6 years ago, no new AI pathfinder projects have begun.

Fifth, upscaling the workforce. The U.S. should invest in rapidly training the DOD workforce for AI. Scale has already worked on this with the DOD to tackle this challenge head-on.

In St. Louis, we established an AI center which has created more than 300 AI-focused jobs, ranging from entry-level labelers to machine learning engineers with advanced degrees.

The race for global AI leadership is well underway, and I cannot be more excited to do everything in my power to ensure that the United States wins. It is in moments like this that Congress, the DOD, and the tech industry can either rise to the challenge together or stand idle.

I have included my further remarks in a written statement to be submitted for the record.

And thank you again for the opportunity to be here today. I look forward to your questions.

Thank you.

[The prepared statement of Mr. Wang can be found in the Appendix on page 37.]

Mr. GALLAGHER. Thank you, Mr. Wang.

Mr. Kitchen, you are recognized for 5 minutes.

STATEMENT OF KLON KITCHEN, NONRESIDENT SENIOR FELLOW, AMERICAN ENTERPRISE INSTITUTE

Mr. KITCHEN. Good morning, Chairman Gallagher, Ranking Member Khanna, and members of the committee. Thank you for the privilege of testifying.

I would like to use my opening statement to make three points.

First, I believe artificial intelligence, and particularly emerging capabilities like generative AI, are a national security lifeline for the United States. The national security community has discussed the potential of AI for years, but now it seems these technologies are finally maturing to where they can be applied at scale—with few doubting that they will soon reshape almost every aspect of our lives, including how we fight and win wars.

The importance of AI is felt as acutely in Beijing as it is in Washington. But, until recently, I was not at all confident that the United States would hold the AI advantage. If you assume this advantage comes down to algorithms, data, and hardware, just 1 year ago I would have given the United States the advantage on algorithms, the Chinese the advantage on data, and I would have called hardware a jump ball.

But this deserves another look. Large language models and other generative AIs may be moving the competition back to the American advantage. The U.S. dominates the underlying computer science giving birth to these advancements and we remain the home of choice for global talent.

On hardware, a strong, bipartisan consensus is allowing us to meaningfully constrain China's access to cutting-edge capabilities, like advanced graphics processing units, and even more can and should be done. For example, limiting Chinese cloud services would be an excellent next step.

Finally, on data, while the Chinese economy and people continue to generate a deluge of digitized data, and while the Chinese Communist Party continues to have unfettered access to these data, the promise of synthetic data and the fact that many of the new AI models are indexed on the open internet may blunt the CCP's advantage.

It is my hope, for example, that the Chinese government's political fragility, strict content controls, and general oppression of its own people will compromise or bias much of the data that it collects, diluting its utility and ultimately limiting the development of Chinese AI. At the very least, I think that the United States has an opportunity to surge ahead of Beijing if we are aggressive and deliberate.

But AI offers the U.S. more than bespoke capabilities. Large language models and other generative technologies, if properly realized, could provide an economic base for a new era of American prosperity and security.

For years, we have known that the United States is not investing in its military sufficiently to meet the demands of the Nation. The truth of this has been laid bare, as our defense industrial base struggles to keep up with the demand of the conflict in Ukraine, for example.

But according to one recent study, existing generative AI capabilities could add the equivalent of $2.6 trillion to $4.4 trillion annually to the global economy, and that this estimate would double if we include the impact of embedding generative AI into existing software that is currently used.

The bottom line is this: I believe AI is offering us an opportunity to get our economic house in order, to lay a foundation for our Nation's long-term prosperity, and to build a national security enterprise that is properly resourced.

But finally, while AI offers all this promise and more, it is also has serious national security risks; most acutely, a flood of misinformation and the exponential growth of conventional and novel cyberattacks. By now, we have all seen the photos, videos, and other media generative AIs are creating, and these capabilities have already been democratized. Virtually anyone can create and distribute synthetic media that will undoubtedly be used to undermine American confidence in our democratic institutions.

Similarly, generative AIs will offer hostile cyber actors potent tools for generating and automating traditional and new online attacks. In a world where we are already overwhelmed by online threats, generative AIs will soon pour gas on these fires.

There is much more that I could say on these matters, but I trust we will cover them more fully on the course of this hearing.

Thank you again for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Kitchen can be found in the Appendix on page 53.]

Mr. GALLAGHER. Thank you, Mr. Kitchen.

Dr. Mahmoudian, you are recognized for 5 minutes.

STATEMENT OF HANIYEH MAHMOUDIAN, GLOBAL AI ETHICIST, DATAROBOT

Dr. MAHMOUDIAN. Thank you.

Chairman Gallagher, Ranking Member Khanna, and the members of the Cyber, Information Technologies, and Innovation Subcommittee, thank you for the opportunity today to testify before the subcommittee on the critical issues of machine learning and human warfare: artificial intelligence on the battlefield.

My name is Dr. Haniyeh Mahmoudian, and I am the global AI ethicist at DataRobot. In my personal capacity, I am an advisory member to the National AI Advisory Committee and co-chair the AI Future Working Group. Today, I testify in my individual capacity.

AI holds immense potential and is increasingly becoming an essential component of modern military strategies and operations

with potential to profoundly impact operational efficiency and decision making.

In the realm of cybersecurity, AI can help military protect its network and systems against increasingly sophisticated cyber threats and also assist them in offensive cyber operations.

AI can also play a critical role in predicting and prevention of injuries among military personnel. AI can efficiently track real-time fatigue and injuries, which can aid prevention of MSK [musculoskeletal] and other bodily injuries, which, along with consequences, is a major reason for medical disability and consequent discharge from the service.

Thus, it is imperative that the United States expedites the adoption of AI to sustain our strategic military leadership and advantage. While these benefits are significant, it is crucial to ensure that the use of AI in the military context adheres to law and ethical guidelines.

In recent years, insufficient scrutiny of AI and evaluation of AI systems, coupled with a limited comprehension of AI's potential adverse effect, have led to numerous instances where AI, despite being developed with good intentions, ended up harming individuals and groups it was designed to help.

This suggests that consideration of AI ethics have often been relegated to secondary thought when it comes to building and deploying AI systems. However, it is encouraging that the Department of Defense has taken initiatives to develop AI ethics principles that will apply to both combat and noncombat functions.

As former Secretary Esper has remarked, "AI technology will change much about the battlefield of the future, but nothing will change America's steadfast commitment to responsible and lawful behavior."

Incorporation of responsible AI frameworks and fostering trust in AI systems requires consideration of people, process, and technology. Investment in AI and AI ethics literacy for military personnel at all levels is a key step to ensuring responsible and appropriate use of AI.

To successfully adopt AI and have it at scale at the Department of Defense requires that the Department implement AI governance frameworks and adopt risk-management processes to manage and mitigate risks associated with AI.

One of the challenges in adoption of AI in the government, especially in the Department of Defense, is a slow procurement process. As mentioned earlier, AI is an evolving space. Therefore, it is paramount for us to make sure that we have a faster procurement cycle, but ensuring that we also have proper evaluation of AI tools by using robust governance processes.

In conclusion, AI holds transformative potential. However, along with these benefits, it is vital to establish ethical frameworks and comprehensive governance processes that ensure effectiveness, reliability, and human oversight.

Thank you.

[The prepared statement of Dr. Mahmoudian can be found in the Appendix on page 68.]

Mr. GALLAGHER. Thank you to all our witnesses for your thoughtful testimony.

I now recognize myself for 5 minutes.

Mr. Wang, I would like to begin by asking you to respond a bit to some of what Mr. Kitchen laid out in terms of our advantages and disadvantages relative to China in the AI race. How do you see those advantages—relative advantages and disadvantages?

Mr. WANG. So I certainly agree that America is the place of choice for the most talented AI scientists in the world. So we certainly continue to have an advantage there. And the evidence is clear, if you look at ChatGPT, GPT–3, GPT–4, as well as the transformer model that underpins it, all of those were invented in the United States.

When it comes to data, I actually also agree that we have a potential very powerful advantage here, specifically when it pertains to military implementations. So in America we have the largest fleet of military hardware in the world. This fleet generates 22 terabytes of data every day. And so if we can properly set up and instrument this data that is being generated into pools of AI-ready datasets, then we can create a pretty insurmountable data advantage when it comes to military use of artificial intelligence.

Now, I think this is something that we need to work together and actually move towards as a country. Today, most of this data goes unused or is wasted in some manner. We need to fix that to create a longstanding and durable advantage in artificial intelligence data.

And when it comes to computational power, Nvidia, which is the world's leader in chips for artificial intelligence, is an American company. These technologies are innovated and built in America. And so, again there, I think we have an advantage.

Thank you.

Mr. GALLAGHER. And, I mean, you have dealt a lot with the Pentagon. It is a customer of yours. Why is it at present—I know a lot of this is in your written testimony—that it is wasted? What is preventing us from harnessing that data? And I guess, more broadly, what is preventing us—why have we not had new pathfinder projects since Maven?

Mr. WANG. So data is something that is significantly more valuable with the advent of these artificial intelligence algorithms. So, you know, a very simplistic way to look at AI is that you have these algorithms that analyze troves and troves of high-quality data, identify patterns in those data, and then can emulate those patterns going forward.

So we see that with models like ChatGPT which are able to read troves and troves of language data, things that humans have written over years and years. Then, it can emulate how a human might speak in a lot of these instances.

So these artificial intelligence algorithms have made data significantly more valuable than they have in the past. And so it is a new paradigm that the DOD needs to adapt towards. As we all know, the DOD is a fragmented organization. There's many different constituencies and organizations that each have their own approach to data.

And like one of my witnesses mentioned, there's an education process and an upscaling process that needs to happen. Everyone within the DOD needs to understand that data is actually the am-

munition in an AI war. And if we have that recognition as an entire Department, and as a country, I think it becomes very clear for us to take the right actions to actually collect all this data and move forward.

Mr. GALLAGHER. It sounds as though you are suggesting that, with the right leadership and organization, DOD could actually be a leader in this space. I wonder if it could also be a leader in terms of the guardrails that a lot of our constituents are asking us about, right? I think your average American understands we need to win this competition, but is concerned about, you know, uncontrolled AI. And everyone has seen Terminator, et cetera, et cetera.

What is your assessment of the DOD's ethical framework? Is that potentially a foundation that could be built upon, expanded, to ensure we are on the same page within the Five Eyes alliance, within the NATO [North Atlantic Treaty Organization] alliance, and then, gradually bring more and more people into that sort of free-world framework for AI?

Mr. WANG. I definitely agree. I think it is really critical that the United States takes the lead on this topic, particularly as it pertains to ensuring that artificial intelligence is used in accordance with our values and our principles.

The DOD has established ethical AI principles, which I believe are great, and those principles are ones that we should continue to adhere. And I think now it comes down to implementation. How are we going to actually make sure that these principles are followed?

That is where I think a test and evaluation regime is incredibly important and critical to the increased deployment of these AI systems. You know, as the DOD looks to apply AI to every function within its operation, everywhere from warfighting to back-office functions and logistics, we need to have proper test and evaluation mechanisms that ensure that every instance of artificial intelligence deployed follows our ethical AI principles.

So I think we need to set up the framework by which we can ensure all this deployment follows those principles and really lead the world in terms of thinking on how AI can be used in accordance with democratic principles.

Mr. GALLAGHER. I have questions for the other witnesses that I will have to save for a second round.

I recognize Mr. Khanna for 5 minutes.

Mr. KHANNA. Mr. Keating, would you like to go?

Mr. KEATING. Thank you, Mr. Chairman, since I have to do this. Let's see if I can do in 5 minutes here three quick questions, and quick answers, I hope.

Mr. Kitchen mentioned global talent and we have an advantage. But we also have immigration issues here that is hindering that talent. Indeed, should we change some of the immigration barriers that exist to get that global talent here to the U.S., make sure we are not losing that talent to other countries?

Mr. KITCHEN. So immigration policy is outside of my area of expertise. What I would say is that maintaining our access and continuing to be the preferred home of global talent will be essential for national security.

Mr. KEATING. Okay. This question deals with the procurement issue that the doctor mentioned. If you could, it is fragmented, the Department of Defense. Could you give this committee, as a follow-up, some suggestions on procurement changes just within the area of AI? Is that something that could be carved out? Because this is an area of great significance. And you mentioned that, and I agree, is a major, major problem. It is a problem generally, but can we do something specifically with that that you could suggest to this committee?

Dr. MAHMOUDIAN. So one area that we can think about—and I have to emphasize that military is not my area of expertise—but one area that I can bring from the business perspective, because on the business side you also go through—procurement side goes through proof of value or proof of concept.

So one of the challenges that we also see over there is the long process of evaluation, which, if we have standard procedure in place, these type of processes, these type of evaluations, as long as they are standardized, it can go much faster.

Mr. KEATING. Thank you.

Mr. Wang, you are familiar, though, on the military side. Can you follow up on that?

Mr. WANG. Yes. I think there have been immense strides in building fast procurement methods for the Department of Defense. Notably, the CDAO, the Chief Digital and AI Office, has set up a Tradewinds program which is one of the fastest procurement methods for new technologies, new and innovative technologies in the DOD.

DIU, as an organization, has also been actively partnering with many innovative tech companies in bringing their technologies into the DOD.

And so there are current programs that I think we can double down on. Both of these instances that I mentioned at the CDAO and at DIU are working. And I think what we need to look towards in the next era of AI is doubling down on some of these fast procurement methods and ensure that we continue innovating.

Mr. KEATING. Is that something that you could follow up with the committee and provide that kind of information, how it could be tailored, or doubled down, as you said, more efficiently, something we could exchange with the military?

Mr. WANG. Of course.

[The information referred to can be found in the Appendix on page 123.]

Mr. KEATING. Okay. Thank you.

Then, just an overview. I think Mr. Wang might be the proper person, but the others can comment in the 2 minutes I have left.

Mr. Wang mentioned that we have a data advantage in the U.S., but we are not capturing all that data. But I think inherently in our democracy with privacy right protections, we are at a disadvantage in terms of how Chinese operate themselves.

And, you know, it can't just be broken down into information, military and otherwise. All that information is valuable that they gathered.

Is there an area where, because of our privacy protections—which is something we shouldn't change in our country—where we might be at an inherent disadvantage with China?

Mr. WANG. So I actually look at our democratic values as an advantage when it comes to artificial intelligence. If you zoom in on the realm of large language models, this is an area where in the United States we have clearly raced ahead, and we have invented much of the technologies. And if you compare that to the current, what we know of how China views this technology, you know, they are likely going to squash a lot of the technology because it is impossible to censor.

I mean, anyone can use ChatGPT and notice that, you know, ChatGPT can say all sorts of different things. In the United States, we have protection of free speech. And so we will continue innovating when it comes to large language models. In China, they view that as a risk to their socialist values. They recently came out with regulations that say that their AI technology has to adhere to socialist values.

Mr. KEATING. That is interesting, huh?

Mr. WANG. Yes, it is very interesting.

Mr. KEATING. And I'm glad I asked that question, and I never looked at that aspect of the answer.

Lastly, quickly, with 30 seconds to go, you know, Vladimir Putin has said whoever controls AI has a huge advantage, but look at Russia right now. Is it fair to say that they are way behind? Is it fair to say that their involvement in Ukraine and what it is doing to the economy and the sanctions are having an effect? Yes or no? Just in 14 seconds.

[Laughter.]

Mr. KITCHEN. Yes, I think there is good reason to suspect that the Russian AI capability, while they may have some basic research, in terms of applied deployment is minimal.

Mr. KEATING. All right. I thank the ranking member for switching his time, so I could go to another hearing.

Thank you. I yield back.

Mr. GALLAGHER. Dr. McCormick is recognized for 5 minutes.

Dr. MCCORMICK. Thank you, Mr. Chair.

And thank you to the witnesses. I wish I had time to talk to you all day because this is fascinating. You are all, obviously, experts. Unfortunately, we get time enough for about two questions and that is about it. So I will go with the most pertinent that you guys actually brought up in your opening statements that I thought was really interesting.

Mr. Kitchen, you just discussed limiting Chinese access to our information, which totally makes sense. We see how they can develop very rapidly when they literally take our information and apply it.

My concern is we have an enormous amount of foreign students at our universities right now in some of the leading technology areas, including AI development. Georgia Tech is right in my back yard. I went to Georgia Tech. I did my pre-med there. And we are literally educating them and sending them right back there. That is access to leading technology in America. Is that what you are discussing when you talk about access or are you talking about in

the industry itself? Or the stuff that is out on the internet? Or is it everything?

Mr. KITCHEN. Thank you, Congressman. It is an important question.

Certainly, there is undeniable—a level of risk associated with foreign, and particularly Chinese, student presence in the United States. However, the research that I have seen by organizations like Georgetown's Center for Security and Emerging Technology actually demonstrates that the vast majority of foreign research students, even Chinese students, actually stay in the United States or, more broadly, in the West, for the course of their career and amplify our capability.

What I'm most concerned about, however, when I talk about Chinese access to data—again, not dismissing an inherent, built-in threat there—is, frankly, their acquisition through purchase of American data through large data stores, but then also things that we have all been talking about and staring at in the face for multiple years now—things like Chinese-owned and operated social media companies like TikTok, where every bit and byte of data that is generated via these applications on Americans' phones is, by law, made accessible to the Chinese Communist Party.

And so while Chinese students and other foreign students may have some type of risk, it pales, in my view, in comparison to the type of data that we are just kind of giving away.

Dr. MCCORMICK. I appreciate that and I can totally understand where that is coming from. My other concern, though, in regards to that—and this is just a quick comment—is that the Chinese government is not stupid, and they, obviously, don't really care about their people more than they do about their government. So when they allow people to come here for education or jobs, I think it is with nefarious intent, and that is my worry. I'm not saying we don't need to educate people from other foreign lands, but I'm worried about it. And worried about anybody who is pushing their people over here, knowing they are not coming back for a reason.

With that said, also, Mr. Wang, you made an interesting statement about investing in AI and how China has got three times more investment in their AI. Of course, the one thing we do have a huge advantage is we have a lot of private people that are investing in AI now, and China doesn't have that. They don't have the capacity to outperform our private industry because they don't have a private industry.

How do we compare when we combine our synergistic efforts between government and private industry with China as far as—and you mentioned, Mr. Kitchen, that in that effect that we allow this freedom of flow and it is not controlled. So it does have the potential to outpace, as long as we put the right guardrails on it when we are talking about our competition with China.

Mr. WANG. Certainly, if you factor in the amount of private sector investment into AI in the United States, that is an incredible sum. You know, large technology companies, the venture capital industry, and now, the sort of global enterprise is investing billions and billions of dollars into AI. And so if you tally all that up, it is an incredible investment into artificial intelligence in the United States.

That being said, I don't think we should rest easy on that, because military implementations of AI are going to be incredibly important. We need to ensure that in this next phase that the U.S. is both economically dominant, but also has military leadership as well when it comes to artificial intelligence.

And so, you know, we need to consider what the overall investment into military implementations looks like, and that is where there is a large disparity. That is where China is investing 3X more. And if you compare as a percentage of their overall investment, the PLA is spending somewhere between 1 to 2 percent of their overall budget into artificial intelligence; whereas, the DOD is spending somewhere between .1 and .2 percent of our budget into AI.

Dr. MCCORMICK. That is a good point. And it is interesting to watch these private industries now in the United States pairing with the DOD to develop a lot of that stuff, which is very cool, including yourself.

I will say, since I am out of time, just that we shouldn't sleep on Iran and Russia, who obviously want to be players. They have used technology in the past to disrupt other countries, and they, of course, love misinformation. So this is something we need to be aware of.

Thank you. With that, I yield.

Mr. GALLAGHER. Mr. Khanna is recognized for 5 minutes.

Mr. KHANNA. Thank you, Mr. Chairman.

Mr. Kitchen, I thought it was interesting that you said that the advantage that China may have because of data is diminishing because things like ChatGPT are based on the entire universe of the internet, which has both good and bad data in it.

And then, Mr. Wang, you said that DOD is really relying on sort of tagged, annotated data. I guess I'm trying to understand, what is the best data that is needed for AI to be effective in military applications? And does China have an advantage on that kind of data or not? And I would love both of your answers on that.

Mr. WANG. So both data are important, both sort of open source data that is accessible on the internet—that is a key data source for large language models like ChatGPT—as well as high-quality, annotated datasets. ChatGPT and its precursor InstructGPT were trained on large quantities of high-quality, expert-generated data. And it is an important data source to ensure that these systems are more trustworthy, truthful, responsible, et cetera.

So both matter, but when you look towards, again, military implementations of AI, the key is, what is the military data that these models are trained on. Right now, the models that are used by consumers and are present in the private sector are trained on, essentially, no military data. As a result, you know, if you would try to apply these without any additional data towards military problems, they would not perform particularly well.

So as we look towards applying artificial intelligence to the military, we need to have military AI-ready datasets that are ready for this kind of deployment. When it comes to that kind of data, I think probably today you would say it is a jump ball. I think that PLA is looking deeply at this issue and that DOD is looking deeply at this issue.

But we have all of the fundamentals to have an insurmountable advantage because the DOD generates 22 terabytes of data—far more data that the PLA generates—on a daily basis. So if you can instrument this data into one central repository, we can come out ahead.

Mr. KHANNA. So their being—and then I want Mr. Kitchen's comments.

Their being a surveillance state of just getting data from all their citizens is not really going to be helpful for the military datasets that are needed to solve military problems. Correct?

Mr. WANG. It would be of very limited help, and military data is, you know, orders of magnitude more valuable for military problem sets.

Mr. KHANNA. Mr. Kitchen.

Mr. KITCHEN. Yes, sir, I completely agree with what Alex is saying. I think the application matters. So in military applications, particularly anything that would be tactical or kinetic, military-generated, well-curated data is really going to be the key differential.

The point that I was trying to raise when I mentioned the data advantage perhaps swinging back our way, it is in one sense aspirational. Part of the hope of generative AI is that over the course of time we will be able to generate what is called synthetic data. So instead of data that has been produced via normal economic activity or military activity, that GenAI, generative AIs, are able to then begin generating synthetic datasets that would be useful for training.

I suspect that we are, number one, not there yet; and number two, that those datasets will be helpful for broad economic application, but not at all the type of—it will be supplemental to the type of military applications that Alex was discussing.

Mr. KHANNA. Thank you.

Dr. Mahmoudian, thank you for your testimony.

I know Secretary Esper had introduced an AI framework/guidelines for DOD. I'm not sure if that has been updated now. Are there things you would want the DOD to do more in terms of the ethical guidelines/framework for the use of AI?

Dr. MAHMOUDIAN. So the DOD, as I mentioned, they already have AI ethics principles in place. So one comment that I would have about that is how we can make these frameworks from abstract to a practical form of view. And that comes with the education of the personnel—to make sure that personnel understand what these principles mean and how they can actually, in practice, apply to their use cases that they are working on. So that is a first step.

The second step is the implementation of AI governance. So when you are talking about policies, processes that their AI governance would have, those measurements that would be part of this process would include the principles that they have.

So it is all about people and the process, and obviously, the technology. How we are going to measure those risks that we may identify in a use case. These are all part of the technology aspect of it. Design the technology in a way that it would provide explanation of why the system made certain decision.

And I'm out of time.

Mr. KHANNA. Thank you. Thank you.

Mr. GALLAGHER. Mr. Gaetz, Esquire, is recognized for 5 minutes.

Mr. GAETZ. Mr. Wang, thank you for bringing into sharp relief the extent to which we have to think about all of these weapon systems that we have in contested environments as data collection platforms—almost primarily when it comes to integration with AI. And I took great interest in your call to the committee that, you know, we not waste that exquisite data that is being collected.

What advice would you have for the committee about shaping some sort of access or utilization regime for the data that we are currently wasting?

Mr. WANG. I think this is one of the most important things that we can do to set up America for decades and decades of leadership in military use of AI. Right now, a lot of this data goes onto hard drives, and what ends up happening are the hard drives are either overwritten with new information, so the old data gets deleted effectively and lost, or these hard drives go into sort of closets or places where they never see the light of day.

So first is instrumenting the data to sort of flow into one central data repository. The CDAO has a legislative mandate to do so and set up a central data repository for the DOD. So I think that is of critical importance.

And then, this is a whole-of-DOD issue. Every service, every group, every program needs to be thinking about how can they—all of the data that their programs are collecting and that are being generated within their purview, how can they ensure that all these datas flow through into one central data repository, and then, are prepared and tagged and labeled for AI-ready use down the line.

Mr. GAETZ. And it would seem as though, under the normal construct of a mission set, someone might reasonably be stovepiped away from the broader utilization of some of that data. So it almost seems like something that is an appendage to a mission set. Very hard to weave it in because, as you are collecting data in contested environments, it could be for all kind of reasons and all kind of help.

I wonder aloud, what will be commoditized first, the processing capability on some of these platforms or the data itself?

Mr. WANG. Well, I think you are right that this is, you know, data is a new asset for this new regime of AI warfare. Data truly is the ammunition that will power our future efforts in the military. So it is a new paradigm to think about data as a key and central resource versus, as you mentioned, an appendage that sort of doesn't feel particularly critical to the future operation of our programs.

Mr. GAETZ. Yes, you know, we do all kind of domestic policy/military policy around who can access rare earth minerals; who can access various forms of energy. And I wonder if in the future a nation-state's access to exquisite datasets that have been properly stored and collected are viewed just as precious.

I also wanted to reflect on the smartest hour I ever spent. It was listening to Elon Musk with our chair and ranking member discuss some of these issues, and I would encourage anyone watching this who has an interest in the issue—hard to find a conversation on

the internet with a higher average IQ [intelligence quotient] across the board than that one.

But what Mr. Musk presented as an argument was that China understands that AI control of governance is equally a threat to them and to the United States. And so Mr. Musk's argument was, we really are ideal partners with China because we share a common goal to not have the AI robots ultimately take over our governance.

And our chairman offered, I think, a pretty strident critique of that perspective saying that, while we view China as typically thinking long term in the short term, they are more "Team Communistic Genocide" than they are "Team Humanity."

So I was just wondering if, because you had so much in your written testimony about your time in China, and how that shaped your perspective on the ethics of all this, do you think China sees an overlap of interests with the United States on this? Or do they see us as explicitly an arm's length competitor?

Mr. WANG. I think it would be a stretch to say we are on the same team on this issue. I think that, if you look at the last generation of AI, computer vision technology, the way that China approached it was utilizing it—building an industrial base that was government-funded to immediately build advanced facial recognition technology for the suppression of their population and the suppression of Uyghurs—ultimately sort of tightening the grip of their totalitarian regime.

I expect them to use modern AI technologies in the same way to the degree that they can. And that seems to be the immediate priority of the Chinese Communist Party when it comes to implementations of AI.

Mr. GAETZ. We will count you on Team Gallagher, not Team Elon, on that.

And just a question for the record. I would love to know everyone's perspective on what the most important alliances the United States is involved in when it comes to these AI regimes. Is it AUKUS? Is it Five Eyes? Does NATO have a role to play in the ethics around this? I would love to submit that for——

Mr. GALLAGHER. Well, I will break the second commandment, which there is a corollary—if you say something nice about me or the ranking member, you get more time.

I just quickly, what is the answer to Mr. Gaetz's question? That is an interesting question.

Mr. WANG. I think they are all important. I would probably start with Five Eyes, given the strength of our partnerships within that group.

But, you know, as we look towards artificial intelligence as a global technology that will shape much of the future of the world, I think we need to form as many key partnerships as possible to ensure that particularly the governance of this technology, both for—certainly for military use, for use in intelligence, and for use sort of in commercial purposes are adhering to the democratic values that we have as a country.

Mr. GALLAGHER. Quickly, Mr. Kitchen.

Mr. KITCHEN. From a traditional security alliance, I would say Five Eyes and NATO will be critical. However, I would say that the

broader economic partnership with our friends and allies in the European Union is going to be critical long term and is going in the wrong direction. Happy to talk about that more.

Mr. GALLAGHER. Quickly, Dr. Mahmoudian.

Dr. MAHMOUDIAN. I'm echoing the sentiment that the other witnesses had. Later in the year, we are going to have our first AI summit that is happening in the U.K. [United Kingdom] So we need to expand these types of alliance, as mentioned earlier, with our allies on the area of AI.

Mr. GALLAGHER. Great.

Ms. Slotkin is recognized for 5 minutes.

Ms. SLOTKIN. You know, I would just say, just following on that last question, with Five Eyes, we have had generations of learning how to share with each other and become interoperable. I don't actually know if we have data-sharing arrangements when we don't have a joint platform. And it is just fascinating to just think about, like, getting those arrangements in place and sharing data, given the value is going so precipitously up on it.

So, you know, I would say what we are doing here up on the Hill, with the help of industry who is invested in AI, is like admiring the problem, right? We are all talking about the problem of, like, this new tool that we know has real potential, but also has potential real downsides. And so how do we govern it? And our constituents are asking us, like, what are the ground rules on this new technology because it sounds scary?

And I would commend the Joint Artificial Intelligence Center at DOD for putting up some basic, really 40,000-foot guidelines on being responsible, and equitable, and traceable and reliable, and governable, but it is like it is real top-level stuff.

But we are up here, you know, the flip-phone generation, trying to figure out how to govern AI, and it is complicated. But could you give us a sense, sort of in colloquial English, of what keeps you up at night about the military use of AI? If China is investing at least 3 times, and in some cases 10 times, the amount that we are, what is the number one thing that you feel like, you know, kind of worst-case scenario, if we go unchecked, we could see in the next decade?

Mr. Kitchen, you are shaking your head.

Mr. KITCHEN. Thank you.

While there are certain risks of what we would call kind of bespoke threats, I think the most acute challenge that we are likely to encounter in the near term is a simply more effective and efficient enemy.

So the chairman referenced a quote from the Korean war. I will raise him with another one from General Pershing who said, "Infantry wins battles, but logistics wins wars."

And I think supply chain and military logistics, and a lot of what we call kind of back-office military capacity, is what is likely to be reshaped by AI in the near term, which can sound innocuous and not so scary——

Ms. SLOTKIN. Not after Ukraine. I mean, not after watching Russia in Ukraine. I will be happy to invest in more improved logistics, given what we have just seen, the buffoonery in the Russian military.

But I just want to make sure Mr. Wang has an opportunity. That is a good one and it is not a scary thing. It is just a more capable and competent adversary, whoever they are.

Mr. Wang.

Mr. WANG. I would certainly agree that the application of AI to back-office functions, logistics, and just overall optimization is really critical. If you look towards, you know, the areas where the PLA is investing into artificial intelligence, it is for autonomous drone swarms, whether that be aerial, subsurface, or ground. They are investing across all fronts. They are investing into adaptive radar systems which jam and blind U.S. sensors and information networks. So they are investing across the whole spectrum in artificial intelligence to sort of set the new tone of warfare with this technology. And so we need to be investing across the slate.

That being said, I worry as well about the risks in deploying these AI systems without proper guardrails. And for me, it really comes down to implementation, which is test and evaluation.

So how do we know that, for all of the artificial intelligence systems that the DOD is likely to deploy over the next few years and the next decade, how do we ensure that each of these AI systems adhere to the DOD ethical AI principles, as stated.

So I think it needs to be a standard part of the procurement process, is a test and evaluation mechanism to ensure that every instance where a program within the DOD is looking to use artificial intelligence, that we have the right testing and evaluation to ensure that it adheres to our guardrails.

Ms. SLOTKIN. And I know that the Department is working hard on this data-labeling problem and trying to—it is an enormous task to ask what tends to be a stovepiped organization to share data, make it available, label it, make it usable.

If you were king or queen for the day and could get them to do one thing on reliability of data and availability, what would it be?

Mr. WANG. I would say, first, establishing the central data repository, and then creating a plan by which as much of the 22 terabytes of data generated a day goes into that central data repository. And then creating a plan by which as much of that data is processed and labeled and annotated to be AI-ready as possible.

You know, these are all multiyear efforts that are not going to be solved tomorrow at the snap of a finger. They need to be solved through long-term planning and long-term coordination.

Ms. SLOTKIN. Great.

Thank you very much. Yield back.

Mr. GALLAGHER. Mr. LaLota is recognized for 5 minutes.

Mr. LALOTA. Thank you, Chairman. Thank you, Chairman Gallagher, for your leadership on this issue and to our witnesses for helping to inform Congress on these important issues. Along with my colleagues from both sides of the aisle, I am concerned with the rapid advances in artificial intelligence and machine learning, specifically with our adversaries like China.

What concerns me most is the Chinese Communist Party has been making great strides and intends to be the world's leader by 2030. And while we here in the United States have made significant improvements in recent years and we continue to advance,

thankfully, we still have much work to do when it comes to ensuring the DOD is adopting and deploying these capabilities properly.

With that, I wanted to give a shameless plug for one piece of legislation that I have for the AI space. My legislation would require the Office of Management and Budget to issue guidance to Federal agencies to implement transparency practices relating to the use of AI and machine learning, specifically when AI is being used to supplant a human's decision making impacting American citizens.

While my legislation focuses more broadly, I wanted to ask for your thoughts on where the DOD currently stands when it comes to AI and machine learning. Where is the U.S. compared to our adversaries such as Russia and China with respect to fully implementing the latest capabilities? Are we years ahead? Are we on par? Are we years behind? And what are some ways you would plan for the DOD to speed up the adoption and implementation of AI effectively at the Department?

Mr. Wang.

Mr. WANG. So when we look at the new technologies like large language models, like ChatGPT, that have sort of really come to light over the past year, I think that is a jump ball. This is a new technology that we need to implement as quickly as possible, they are trying to implement as quickly as possible, and we will see how that develops.

If you look towards the last generation of AI technologies, which is computer vision and AI for things like facial recognition, this is an area where the original techniques were invented in the United States, but then China quickly raced ahead. So they built an industrial base within their country, funded it with government money to build facial recognition technology, which they deployed throughout their country to suppress Uyghurs and overall, you know, tighten the grip of their socialist regime.

If you look today at the leaderboards for computer vision AI competitions globally, Chinese companies, Chinese universities, dominate compared to American institutions. So if you look at that as a case study, the Chinese system clearly has an ability and a will to race forward when it comes to artificial intelligence deployments.

Now, as we look towards this next field of large language models, we have reasons to be optimistic. You know, China is going to be more reticent to invest into large language models because they are difficult to censor. They released recent regulation on—that said that AI needed to adapt to their socialist principles, which I think is a clear limitation if you have an AI that can, you know, sometimes misspeak, like ChatGPT.

So we have reasons for optimism. And again, the DOD produces more data than the PLA, by orders of magnitude; we generate 22 terabytes of data every single day. And so if we can properly build an advantage here, it will be quite durable.

Mr. LALOTA. Mr. Kitchen, would you add something to that? Where is your scorecard at? Are we behind? Are we ahead? Are we on par?

Mr. KITCHEN. Well, I would say that the two global powers where the competition matters most, historically, is between the United States and China. As I mentioned at the beginning of my testi-

mony, a year ago, I had very real concerns as to how the United States was going to be able to maintain its AI advantage.

But precisely because so much of the conversation around AI—legitimately so—the public conversation focuses on the risks and the kind of unknown, again, meaningful conversations. I do think—just analytically, I do believe that we have a moment to reassert American dominance in a way that really matters, that some of the things that I would have called a drag on our development and deployment from a national security perspective are actually lessening, and that if we realize this technology deliberately, then we can seize the advantage, and not just seize the advantage now, but actually build an advantage that will be meaningful over the long term.

And I think that we should do everything we can to do that.

Mr. LALOTA. Thanks.

And with 30 seconds to go, Doctor, I will ask you the last question. What are the risks that this committee, and the Department, should be aware of? And how do we address those risks as we leap forward?

Dr. MAHMOUDIAN. So, when it comes to risk there is obviously a fallback if the United States falls behind with regards to the advancement of AI in military. So the main area that we need to focus on is to make sure that we do have the advantage in the research, investing in the research, especially in the military side, and making sure that we are still a leader in the area of R&D [research and development] in AI.

Mr. LALOTA. Thanks.

Chairman, my time has expired.

Mr. GALLAGHER. Mr. Kim is recognized for 5 minutes.

Mr. KIM. Thank you, Mr. Chair.

Thank you so much for coming on out and talking to us today. We spent a lot of time today talking so far about who has got the development edge and where we are kind of building that direction, certainly about competition with China. So I don't want to go over those right now, as they were very well talked through.

Mr. Wang, you talked about in your opening statement talking about how the—some of the main technology of the past being about nuclear development and whatnot sort of shaping that era, and this very well likely shaping our era.

So I wanted to kind of get a sense from you all about what you think proliferation of this technology and possible weaponry would look like. You know, when we were in the nuclear era, which, you know, we still are—you know, we have a situation here where only a very few set of countries have been able to reach that threshold of technology, and proliferation has been, in many ways, kind of tried—effort to be kind of contained in that capacity.

So I guess I wanted to ask you—for me, that doesn't necessarily seem like the kind of setup that we are likely to see over the coming decade or two. What does it look like to you? Are we going to have a situation where the U.S. and China, a handful of countries, are the major developers and gatekeepers to this technology, but the actual weapon systems and technology will be potentially mass deployed and able for purchase by pretty much any nation that is out there?

Just give us a sense of what that proliferation and topography and landscape looks like.

Mr. WANG. I think this is a really good question. You know, I think in terms of impact, artificial intelligence is going to be similar to nuclear weaponry. But as you mentioned, it is a technology that is likely to be ubiquitous.

A, artificial intelligence can be used across every single domain, every single function, every single activity that the military has today, so it is not sort of contained as one individual weapon. And it is a technology that is increasingly becoming a global technology.

A few months ago, the UAE [United Arab Emirates] announced their own large language model that they had built called Falcon 40B. They actually open-sourced that model to the world so that anybody on the internet can go and download that model, that large language model, for use. We are seeing with the open-source community when it comes to large language models that this technology is likely to be accessible in some way, shape, or form to nearly everyone in the world.

That being said, I think that is not a reason to, you know, give up hope because of one of the things I mentioned before, which is, for military use cases and military applications, you need algorithms that are trained on military data. And——

Mr. KIM. I mean, Mr. Kitchen, if you don't mind, I would like to bring you in. But would we find a situation where, yes, you know, some country or entity or company is doing that but then able to then sell that type of technology and weaponry to a country or to a group?

You know, Mr. Kitchen, I would like to also get your thoughts on potential for rogue actors, non-state actors, to be able to get this type of technology, to be able to utilize it. So, if you don't mind, give us some of your thoughts.

Mr. KITCHEN. So I agree with Alex in the sense of this technology having the same strategic impact of something like nuclear weapons. But one of the peculiarities of it is that this technology is overwhelmingly being developed in the private sector for commercial applications, unlike nukes.

And so one of the implications of that is that, because of that and the fact that so much is done via the open-source model, it is instant proliferation. It is available, in terms of the underlying technology and capacity.

But it is going to be the applications, the particular applications, that really make the difference when it comes to capability distinctions. And that is where Alex's points about the United States having a potential advantage on military data—right? How we apply the underlying capability is really, really going to matter. And that is where the advantage comes to us.

Now, when we think about non-state actors or kind of rogue actors, I think it is—I think where the most acute challenge there is probably on novel and traditional cyber exploitations of these capabilities. So the ability to generate malicious code and automate it and deploy it is now going to be democratized to a level and at a scale that is going to be difficult.

Mr. KIM. I want to just get one last question. Doctor, to bring you in on this, you know, when we talk about this proliferation, seeing

the potential for non-state actors and others, I guess, you know, we talked about some of these frameworks. The U.S. needs to lead the way. But should we be thinking about an actual international agreement here, an international treaty? What kind of structure should we be building towards to give our ability to try to structure that as a whole?

Dr. MAHMOUDIAN. I completely agree. We need to think about both the domestic side—so within the United States, we need to think about how we should be governing these type of technologies, understanding its risk and having mitigation process in place. But we do need to work with allies as an international—at the international level.

Mr. KIM. Okay. Thank you.

I yield back.

Mr. GALLAGHER. Mr. Fallon is recognized for 5 minutes.

Mr. FALLON. Thank you, Mr. Chairman.

I just want to follow up real quickly with Mr. Kitchen. Yeah, I think ransomware is an issue that—it is a huge problem already, and it is one that largely goes under the radar unless, you know, Colonial Pipeline is hit or something, JBS. And that is—everybody talked about it for a week and then forgot about it and acted as if it is not a real problem, which it is when you have friends in industry, small companies—100, 200 people—that are getting hit.

Half-a-million-dollar ransoms now are being asked, or million-dollar ransoms, when a lot of the times, it was 50 grand a few years back. Do you think that with AI, are we going to face, as you just mentioned—but I want you to expand on it—an explosion in ransomware when you say it is democratized?

Mr. KITCHEN. I think that is certainly one of the potential implications. Honestly, I think one of the key developments over the last 2 years that has constrained ransomware to the degree that it has been constrained is the war in Ukraine, that many of those cyber syndicates that were prosecuting those attacks have been repurposed by the Russian government for attacks in Ukraine and elsewhere.

I think, if and when that ever slows down, we are going to feel the surge again. And I think that that surge will absolutely be enabled by generative AI because one of the key areas—there is a study that says that there are kind of four key areas that will constitute approximately 75 percent of the economic increase coming with GenAI. One of those is in R&D, and in software development being the other.

And so I think that applies, unfortunately, equally to the bad guys as it does the good guys.

Mr. FALLON. Yeah. Nobody has ever accused the DOD of being highly efficient. They are large. But when you have inefficiencies, you are talking about wasting billions of taxpayer dollars. Particularly when we are in a competition with China, that is even more troubling, and we need to address it.

We might envision AI with future wars being fought by robots and such, but within the walls itself, these walls, Mr. Wang, in your opinion, can the Department of Defense use AI to extract efficiencies in programming and budgetary activities?

Mr. WANG. For sure. One of the areas that we have already worked with some of our DOD customers on is using artificial intelligence and large language models to help digest requirements that are given by the DOD.

There are so many groups within Department of Defense that are generating requirements, and matching those requirements up with capabilities in the private sector or new capabilities that the DOD develops is an incredible efficiency—potential efficiency gain.

There is hundreds, if not thousands, of applications like that of artificial intelligence towards making the DOD a more efficient organization. So I am incredibly optimistic about the ability to use AI, whether it is in logistics, back-office, you know, in personnel-related matters, to build a more efficient force that wastes fewer resources and ultimately is able to have more force projection capability.

Mr. FALLON. Think that the same thing holds for, you know, increased accountability with DOD contracting and spending?

Mr. WANG. I think that there is—you know, if you think about what the limitations are or what the challenges are, it is in processing huge amounts of information and data that is being generated by the DOD to, you know, understand not only how funds are being used but also understand what the capabilities that are being generated are.

And so if you think about that problem set, it is one that is naturally suited for artificial intelligence and for the use of these large language models.

Mr. FALLON. Doctor, you know, when you talk about AI, my mind starts to bend and hurt and break a little bit because it is just so intriguing. But when we just talk about basic concepts of some of the technology we have grown accustomed to, like with social media, some folks, believe it or not, in this building, on the other side of the building, don't grasp even those—I mean, I remember a major State's governor saying that we should use Tweeter more, didn't even get the name right.

And one of the Senators I think I remember saying, like, "How can they post a picture on the line?" Things like that. So while that is funny, it is also troubling that if they are not grasping basic concepts, and you talk about AI, which is this stuff on, you know, hyper-steroids, how do we go about best educating our colleagues and the American public on AI and assuage some of the fears associated with it?

Dr. MAHMOUDIAN. So when we are thinking about the education side of it, we need to understand that this education needs to be tailored towards people's needs. So depending on their roles, depending on their responsibilities, we need to tailor that education for them.

To give you an example, for senior leaders who may not be technical, we need to come up with an education that lets them know what AI is, exactly to your point, what it is capable of, what its limitations are, versus someone who is technical. Let's say a data scientist. For them, that would be a different story. We can have a more technical education for them, but also having this tech education in a continual form as AI evolves.

Mr. FALLON. So almost like how it can help them specifically and make their lives a little bit better.

Dr. MAHMOUDIAN. Exactly.

Mr. FALLON. Yeah.

Thank you, Mr. Chairman. I yield back.

Mr. GALLAGHER. Mr. Ryan is recognized for 5 minutes.

Mr. RYAN. Thank you, Mr. Chair.

Good morning. Thank you all for being here and for your insights. I wanted to build on some of your—to start building on some of your written testimony, Mr. Wang. You talked about data as the ammunition in AI warfare. You talked about what some of our adversaries, particularly China, are doing.

And then you were—and I appreciate it—candid about areas where we need to improve. Can you talk about, based on your specific experience and your companies working with DOD, who is doing relatively better? What are the lessons we can learn in terms of—and also, if you could talk a little bit about CDAO and how you see that intersecting here so that we can recognize the imperative around wrapping our arms around our data better.

Mr. WANG. Certainly. So the groups that we work with, by nature of, you know, us generally working with the more forward-leaning groups within the DOD, are forward-looking. They are extremely innovative, and they have incredible—in terms of taking on this technology as a key part of their go-forward strategy and building impressive capabilities.

So, you know, we have worked with many of the early programs in the DOD for use of AI. And by and large, we have been—I have been incredibly impressed. That being said, I think now is an opportunity for us to build on those successes and really take this moment in the technology and speed up our deployment.

It is incredibly important that we build on our past successes, that we are able to more scalably deploy this technology across the entire DOD rather than being limited to, you know, a few innovative cells within the DOD.

As I mentioned a bit ago, the DIU and the CDAO have been some of these areas, some of the groups within the DOD that have been able to have fast procurement cycles and generally innovate when it comes to use of artificial intelligence. But that needs to happen across the entire Department of Defense.

Lastly, just on the CDAO, I think they have done—you know, it is a recently established organization, but they have done a good job of pushing forward in building, you know, the right—pushing forward the topic of data labeling and the central data repository for the DOD. And now I think we need to ensure that that actually happens in terms of collecting this 22 terabytes of data that are being generated every day.

Mr. RYAN. Thank you.

And just to build on that and bring in anyone else who wants to add here, is it even possible to do that from the top down? I mean, I understand the importance of setting the right tone and direction. But if we think that creating a new office is—it is necessary, but I would argue not sufficient, to really—if we are serious about wrapping our arms around this, it should be emphasized and trained and reinforced that—much more broadly.

Do you agree with that? Any ideas from anybody on how to do that, particularly looking at how others, adversaries or allies, are doing it?

Mr. WANG. A combination of top-down and bottoms-up is necessary here because the individuals who are making the decisions of, you know, when they get a new hard drive off of a military platform and they need to make the decision on what they are going to do with that hard drive, we need all the way down to that individual to understand that hard drive is full of data that will fuel the future of American military leadership.

And so they need to understand that as viscerally as we do from a tops-down perspective within the CDAO or the—you know, within this conversation. So it requires a whole-of-DOD approach to be able to properly achieve this outcome.

Mr. KITCHEN. Congressman, the one thing I would add is that as we tackle these difficult challenges—and they are legion—that just from a mentality standpoint, I would encourage Congress and the U.S. Government to approach these as challenges that have to be managed, not solved.

If we make the perfect the enemy of the good, if we try to find the exquisite solution, we will so delay ourselves as that we will miss the opportunity. And that's one of the kind of key narratives I am really trying to emphasize, is that we really do have a meaningful strategic opportunity. And these guardrails and everything, they matter. They really do.

But as we approach these things, seizing the opportunity, I think, is probably one. And then doing it well and carefully is a part of that, but it cannot be the goal by which we have to leap over before we begin.

Mr. RYAN. I appreciate and agree.

Just very briefly, Dr. Mahmoudian and anyone else, particularly talking—you hit on it all a little bit, but—we are talking about DOD, but how—your sense of, in the research realm, academic realm, how are we doing there? What can we do better? I think I could guess, but——

Dr. MAHMOUDIAN. So we can definitely—when you are investing in the research side of it, it opens the door for us on the innovation side to also invest in research on the safety aspect of it, on these guardrails that was mentioned.

So we need to—when we are investing in the research, we need to consider both in parallel in order to make sure that we are always ahead of it.

Mr. RYAN. Thank you.

I yield back, Mr. Chair.

Mr. GALLAGHER. We will now move to a second round of questions. I will begin by recognizing myself for 5 minutes.

I want to return to Mr. Gaetz's question about key allies in the AI competition. You all mentioned, you know, our most obvious allies. I mean, I think you are right. I am not detracting from that answer—Five Eyes, NATO, EU [European Union].

I would like to invoke Jared Cohen's concept of sort of geopolitical swing states, perhaps countries that may not fit neatly within the free world paradigm. What are the emerging AI superpowers that we may not be thinking about, or let's just say states

that punch above their weight when it comes to AI, that we need to be cultivating and ensuring they are not Finlandizing in the Chinese Communist Party direction?

I will start with you, Mr. Wang.

Mr. WANG. I do think it is really important, you know, as we—as AI sort of promises to be one of the most important technologies both economically and militarily, there are a myriad of countries that are all getting involved.

Kind of as I mentioned, the UAE has a very dedicated effort towards artificial intelligence. They have open-source models. You know, they are continuing that series of developments towards building bigger and more powerful AI models. We don't know if they are going to open-source them, but we will see. I think it is important that, you know, as they develop those, that we try as hard as we can to make sure those follow our principles and our governance regimes.

India is another key country, obviously, you know, very critical when we think about geopolitical allies. But also as you think about their developments in AI, they have an incredibly active tech sector, and they have stated efforts to develop large language models within their country.

So, you know, these are some of the countries I would say that, from an AI perspective, seem to be racing ahead and ones that we want to ensure are thinking about artificial intelligence and its impacts in the same ways that we are as a country.

Mr. GALLAGHER. Mr. Kitchen.

Mr. KITCHEN. I would agree completely. I think this affects the way we think about our relationships. So right now our technology supply chain is distributed in such a way as to where there are critical vulnerabilities. Many of the key nodes are deep within Chinese sphere of influence.

And where I think we are going to be going is we are going to try to build trusted technology ecosystems amongst trusted partners and allies; that the idea is that we identify particularly Western democracies as being the type of organizations that we can partner with so that we have mutually beneficial trade and technology relationships that are the core of future national security partnerships.

That requires, however, a common purpose and common understanding of the opportunities and the challenges. One of the things I am most concerned about is where many of our friends and allies are in the European Union particularly on this issue. So my point there being that when we think about military interoperability in these types of alliances, we also need to understand that military interoperability is going to be predicated on regulatory interoperability.

And that is where we have a real gap between us and some of our key friends. The European Union seems to have concluded that to build their own domestic technology base, they have to deliberately constrain, and at times even decouple, from the American technology base. And that will not work for our shared purposes and is going to be a real problem going forward.

Mr. GALLAGHER. Good point.

Dr. Mahmoudian.

Dr. MAHMOUDIAN. So I completely agree with other witnesses with regards to alliance. One of the things that we need to understand, also, that for those type of swing states that was mentioned, we need to also think about how we can align ourselves to them to make sure that their advancement in AI is also aligned to the United States so we would have that alliance with them, rather, while we are ensuring that we are still the leader in this space.

Mr. GALLAGHER. Mr. Kitchen, you mentioned in written and oral testimony that we—on hardware, we have a strong bipartisan consensus allowing us to constrain China's advancement.

There has been some suggestion—and maybe put on the Select Committee on China hat here—as we engage with Silicon Valley leaders, that while we admire the GPU [graphics processing unit] export controls—in fact, we're able to bring Japan and the Dutch along with us was great, and I give the Biden administration credit for that—there is loopholes whereby they are still able to access a tranche of these sort of second-most-advanced chips right now.

I am curious for your comments on that and, Mr. Wang, yours as well. And I recognize I have run out of time here.

Mr. KITCHEN. Yeah. So this goes to my previous point about an iterative process. I think that you were referencing the October 7 rules, the export control on integrated chips. That was the first tranche, and now we are beginning to kind of optimize and tighten those controls.

It is not a surprise that government and industry are doing a bit of back and forth on this. I think there is a growing recognition between both stakeholders that action is necessary, and now we are trying to find the right way forward. I have high confidence that we will do that.

Mr. GALLAGHER. Quickly, Mr. Wang.

Mr. WANG. It is true. You can see reports that ByteDance and other Chinese companies have bought billions of dollars of GPUs in the past, you know—in this year so far. So it is something that we need to be extremely careful and vigilant about.

Mr. GALLAGHER. Mr. Khanna.

Mr. KHANNA. Thank you.

When Chairman Gallagher and I had that conversation with Elon Musk, he said that AGI [artificial general intelligence] was 5 to 6 years away. I was surprised by that timeline. What is your sense of how long we are from AGI?

Mr. WANG. AGI is an ill-defined concept. And, you know, I think many——

Mr. GALLAGHER. Could you define it, since we are not doing acronyms? You are the guy. Sorry.

Mr. WANG. AGI stands for artificial general intelligence, you know, the idea that we would build an AI that is sort of generally intelligent in the way that humans are. It is not a super well-defined concept because, you know, even in using the current AI systems, you will notice clear limitations and issues and challenges that they have with doing even things like basic math.

AGI as a concept is an enticing one that we in Silicon Valley talk about a lot, but I don't think it is very well defined and not something, certainly, that should meaningfully affect how we think

about, you know, putting one foot in front of the other for not only economic leadership as well as military leadership.

The reality is that the technologies today—large language models, computer vision technology, and other AI systems that are being developed and deployed today—have immense bearing on the future of our world, whether that is from an economic perspective or from a military perspective. And that is why I think it is important that we set the foundations today of investing into data, investing in testing and evaluation, to set up the foundations for long-term success.

My last comment as it comes to AGI prediction timelines—I think this is often a way to sort of distract from the current conversation, which is, in my mind, very important.

Mr. KHANNA. Mr. Kitchen or Dr. Mahmoudian?

Mr. KITCHEN. Yeah. I think Alex is exactly right. The idea of artificial general intelligence—I think what we will be seeing is increasingly agile and capable foundation models, or these types of generative AI capabilities, that are going to be more broadly applicable.

So one of the features of these foundational models is something that is called emergent capabilities. It is the idea that we created this algorithm or this foundation model to be able to do a particular task, and lo and behold, it actually can do this other thing without having been trained to do so. So we are going to see that. That is a common feature.

But I would say that the timeline that was given to you about artificial general intelligence in the next 5 years is aspirational.

Mr. KHANNA. If it is good.

Dr. MAHMOUDIAN. Similar to the previous comments, it is aspirational. But what I would add to that is we are headed to that direction. We see, as mentioned, with regard to foundation models, these type of models that can provide tasks that they were not necessarily trained on, but they can generalize to some extent.

However, while we are heading into that direction—obviously, not in 5 years—but we need to also invest—while we are investing on the research side of it, we also need to invest in the guardrails, the safety aspects of it, to make sure that we are able to mitigate the risks that we are anticipating with regards to artificial general intelligence.

Mr. KHANNA. Maybe I will quickly ask my last question, which is, do you think we need any DOD clearance for any types of AI like we have for nuclear technology? There are safeguards. There is only so many people who can get access to it.

Mr. Wang, is there anything analogous in the AI space?

Mr. WANG. So as we think towards military AI systems, so much of the next generation of capabilities are going to need to be built and trained on top of already classified data. So there is already an existing sort of structure and regime to protect any models that are trained on classified data, whether it is at the secret or top secret or even beyond level, to ensure that those capabilities sort of stay limited to certain audiences and state controlled.

I don't know if we need to build even more on that, but I think that it is certainly true that most of the exquisite capabilities that

the DOD looks to build are likely to be developed at the secret or top secret level.

Mr. KHANNA. Thank you.

Mr. GALLAGHER. Mr. Gaetz.

Mr. GAETZ. I am interested in the integration of AI and human performance. We always are very touched whenever there is—we have casualties that are in training or otherwise that are preventable.

What have any of you learned about where some of the potential lies in utilizing AI in integration with sensor technology and other types of human performance capabilities?

Mr. WANG. You know, one of the areas where artificial intelligence, I think, has some of the most greatest promise is in—as Mr. Kitchen mentioned before, is actually in logistics.

So if you look at one of the largest causes of casualties, it actually was in, you know, transporting fuel and other resources for the military. This is an area where autonomous vehicles or even leader-follower setups are able to greatly improve the efficiency as well as reduce casualties for the military and is one of the goals of the Army's Robot Combat Vehicle program that we are collaborating with them on.

As we look further, these AI systems are assistive technologies in—with our Scale Donovan platform, we are able to assist in key decision-making. This is being utilized right now in military planning exercises to help ensure that all of the data and information that the DOD has access to is being integrated into the correct military decisions.

So there is an incredibly bright future, I think, for assistive use of artificial intelligence to make the DOD more effective.

Mr. KITCHEN. This is one of the most exciting things about AI, in my view, is its ability to help expand human thriving. So, many will have seen a commercial with one technology provider whose—their phone could help users who have speech pathologies or difficulties communicate more effectively. The OpenAI—their ChatGPT has a function for vision-impaired individuals where it describes images for them so they can participate in knowledge gain and application.

And then, when we think about in the military context, I mean, it is going to be the AI underlying technology and capability that enables everything from allowing paraplegics to walk again to bring injury prevention and recovery. I mean, the things that this technology—again, I am not an idealist on this, but the promise is real, and what it means for our society just in general, I think, is very promising.

Mr. GAETZ. As the son of a paraplegic mother, that is an inspiring concept.

Doctor, I wanted to ask a little different twist on that question to you. I have talked with my colleague Mr. Khanna to some degree about how we ought to measure the soft-power capabilities of some of these AI platforms. How is it that ethicists are thinking about what it would mean for the United States, as opposed to China, to be the leader in deploying 100,000 AI robot doctors into Africa or Latin America or somewhere else in the Global South?

Dr. MAHMOUDIAN. It is all about how we want to have our values embedded into these AI systems. When we are thinking about these principles, one area that especially the DOD has is these system to be governable. So depending on the level of risk that these systems pose, we want to have oversight.

In some cases, the risk is low, so we may want to let the AI make the decision. Imagine a benign example being recommending a movie that might be bad. But in specific cases, especially the ones that are lethal, we do not want the AI to make the decision. We want human oversight.

We want AI to be used to provide us information, patterns that we may have not seen. So we would use those information, and us humans would be able to make the judgment. So these are elements that we need to consider when we are thinking about these——

[Simultaneous speaking.]

Mr. GAETZ. That will substantially impact scalability and just the scale of being able to deploy the tech, I would think.

Dr. MAHMOUDIAN. If we have comprehensive governance processes, actually, this does not necessarily be viewed as an obstacle with regards to scalability. A robust and comprehensive governance process actually enables us to have standards and policies in place that can easily apply to any AI use case that we have.

So with that foundation of AI governance, we would be able to replicate the process for any AI use case that we have.

Mr. GAETZ. Thank you.

And I haven't given you enough time to answer this question, Mr. Wang, but one of the things that I am sure we would like to explore with you further is, when we get into this test and evaluation paradigm that you keep coming back to in your testimony, that it is important for us to get a concept of what the core principles of that test and evaluation regime would look like. And I hope you will continue to work with the subcommittee on that.

Yield back.

[The information referred to can be found in the Appendix on page 123.]

Mr. GALLAGHER. I am sorry. I am going to do a third round, but it will go very quick. Trust me. And I am going to apply the—what I call the justice test, which is a reference to my 96-year-old grandmother, Virginia Justice. She is very smart but is not even a member of the flip-phone generation, let alone the AI generation.

So I want you to imagine you are sitting across from my grandma. Each have an old fashioned in hand. Her late husband is a World War II vet. You need to explain to her why a—what she needs to know about AI, why this conversation matters both for the future of warfare as well as her life and the lives of her children and grandchildren. What do you say to the great and beautiful Virginia Justice?

Mr. WANG. If we look towards World War II and the last era of conflict, new technologies like the atomic bomb were critical in ensuring that we both had American leadership and that the values that America upholds were able to continue to prosper and set the tone for the development of the world.

We are now embarking on a new era of the world, one in which a new technology, artificial intelligence, is likely to set the stage for, you know, the future of ideologies, the balance of global power, and the future of the relative peace of our world.

Artificial intelligence is an incredibly powerful technology that underpins nearly everything that we do from an economic and military standpoint, and therefore, it is critical that we as a Nation think about how we not only protect our citizens from the risks of artificial intelligence but also protect our ideologies and democracy by ensuring we continue to be leaders.

Mr. GALLAGHER. Mr. Kitchen.

Mr. KITCHEN. Ma'am, there is a new technology that, under the right circumstances, could protect your grandchildren and this Nation, that could make this Nation economically and militarily strong enough to defend its people and its interests, and a technology that in the wrong hands could imperil those same things. And it is really important that your government and industry work together to realize those promises and to mitigate those threats.

Mr. GALLAGHER. Great.

Dr. Mahmoudian.

Dr. MAHMOUDIAN. It is a technology that is pretty much embedded in our day-to-day lives. We are living with it. We are breathing with it. So we want to make sure that this technology that is part of our life has its—our values, the values that we fought for, is incorporated into this technology so we still would have our civil liberties and civil rights as well as using this technology and leveraging it to have a better quality of life.

Mr. GALLAGHER. Great.

By the way, it just occurred to me, though I love being a Gallagher, if I had my mother's maiden name, Justice, I mean, I would probably be President at this point. That is such a better——

Mr. KHANNA. And a progressive.

Mr. GALLAGHER. Well played.

Any other questions? Okay. A bit of housekeeping before we adjourn. I want to enter three things into the record quickly. The first is the article I referenced before by Jared Cohen on geopolitical—the rise of geopolitical swing states, published on May 15, 2023.

[The article referred to is retained in the committee files and can be viewed upon request.]

Mr. GALLAGHER. The second is something that you, Mr. Wang, wrote in November of last year on the AI war and how to win it, in which you say, "We must recognize that our current operating model will result in ruin. Continuing on our trajectory for the next 10 years could result in us falling irrevocably far behind. Why do large organizations often continue on the path to their demise, even if the future is painfully obvious? The reason is inertia. Bureaucracies will continue to glide deep into the abyss for an eternity."

[The information referred to can be found in the Appendix on page 83.]

Mr. GALLAGHER. And then the third is a recent article by Marc Andreessen, which articulates the optimistic case for AI, entitled "Why AI Will Save the World," in which he says, "The single greatest risk of AI is that China wins global AI dominance and we, the United States and the West, do not. I propose a simple strategy for

what we do about this, in fact, the same strategy President Ronald Reagan used to win the first Cold War with the Soviet Union, which is we win and they lose."

[The information referred to can be found in the Appendix on page 97.]

Mr. GALLAGHER. So I ask unanimous consent to enter all three of those into the record.

Without objection, so ordered.

I ask unanimous consent that members have 5 days to submit statements for the record.

And the hearing stands adjourned.

[Whereupon, at 10:31 a.m., the subcommittee was adjourned.]

APPENDIX

JULY 18, 2023

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

JULY 18, 2023

STATEMENT BY
ALEXANDR WANG
FOUNDER AND CHIEF EXECUTIVE OFFICER, SCALE AI

BEFORE THE
SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION
OF THE
HOUSE COMMITTEE ON ARMED SERVICES

"MAN AND MACHINE: ARTIFICIAL INTELLIGENCE ON THE BATTLEFIELD"
JULY 18, 2023

Chairman Gallagher, Ranking Member Khana, and distinguished members of the Cyber, Information Technologies, and Innovation Subcommittee, thank you for the opportunity to testify today on the critical role that artificial intelligence (AI) will play in the future of our military.

I am honored to be here today to discuss why AI is the most critical technology in this next era of warfare and what the United States must do to win.

Introduction

My name is Alexandr Wang, and I am the founder and CEO of Scale AI (Scale). Scale was founded in 2016 with the mission of accelerating the development of AI. I am proud to say that Scale is committed to supporting U.S. national security and that our technology and platforms power the most ambitious AI projects in the world. From our earliest days of annotating AI data for autonomous vehicle programs at General Motors and Toyota, to our work with leading technology companies such as OpenAI, Meta and Microsoft, and the U.S. government, including the Department of Defense's Chief Digital and Artificial Intelligence Office (CDAO), U.S. Army, and U.S. Air Force, Scale has always been a leader in AI infrastructure development.

As someone who has been part of the forefront of AI development for more than seven years, it is exciting to see this technology finally reach its watershed moment. AI has come to dominate every conversation, every headline, and nearly every technological development we see today. At this critical juncture, the United States must recognize the urgency to navigate this new landscape because we risk ceding our global influence, national security, and democracy to an authoritarian regime.

Supporting the U.S. government and the national security mission is deeply personal for me. I grew up in Los Alamos, New Mexico, where my parents were physicists at Los Alamos National Laboratory, the birthplace of a technology that defined the last era of warfare - the atomic bomb. I was keenly aware that an emerging technology, like AI, could completely change global politics and the nature of war.

This is not a new realization or future speculation.

China Recognizes the Importance of Global AI Leadership

Four years ago, in 2018, I went on an investor trip to China that was both enlightening and unsettling. During this visit, I saw firsthand the progress that China was making toward developing computer vision technology and other forms of AI. I was troubled because this technology was also being used for domestic

repression, such as persecuting the Uyghur population. It was evident that the China Communist Party (CCP) had already strategized how to harness AI for advancing its military and economic power. As China President Xi Jingping declared that same year, "[We must] ensure that our country marches in the front ranks where it comes to theoretical research in this important area of AI and occupies the high ground in critical and AI core technologies.[1]"

China deeply understands the potential for AI to disrupt warfare and is investing heavily to capitalize on the opportunity: It considers AI to be a "historic opportunity" for "leapfrog development" of national security technology.[2] As of 2020, China had outspent the United States on AI technology for defense, both in absolute terms and proportionally. China's military arm, the People's Liberation Army (PLA), spent between $1.6B and $2.7B on AI against an overall defense budget of $178B in 2020, whereas the DoD spent only between $800M and $1.3B on AI against an overall DoD budget of $693B for the same period. China is spending between 1% and 1.5% of its military budget on AI, while the US is spending between 0.1% and 0.2%. Adjusted for the total military budget, China is spending ten times more than the US.[3]

This year, China is projected to spend approximately $14.75 billion on AI investments.[4] In contrast, the administration's FY24 budget request included roughly $5.5 billion for AI.[5] While this marks a historic investment by the United States in AI, we must intensify our efforts to outmatch China's rapid advancements.

The reason for this is that the United States is at risk of being stuck in an innovator's dilemma because it is comfortable and familiar with investing in traditional sources of military power. While we are making sense of this technology and conceptualizing a framework for how to use it, Chinese leaders are actively working to use AI to tighten their grip domestically and expand their reach globally. It's time to act. The U.S. must learn to embrace AI innovation before we are disrupted.

---

[1] See, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-calls-for-healthy-development-of-ai-translation/.
[2] See, https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/
[3] See, https://cset.georgetown.edu/publication/harnessed-lightning/
[4]See, https://news.cgtn.com/news/2023-04-10/China-s-AI-market-spending-to-cover-10-of-world-total-in-2023-report-1iSPv1hUlWM/index.html#:~:text=Spending%20in%20China's%20artificial%20intelligence,International%20Data%20Corporation%20(IDC).
[5] See, https://www.pillsburylaw.com/en/news-and-insights/ai-biden-fy2024-budget.html

This urgency is highlighted by the results of an analytic exercise that reviewed thousands of pages of open-source data on the PLA adopting AI.[6] China's capabilities highlighted in the report should serve as an immediate wake up call. "PLA advances in AI and autonomy will create new vulnerabilities for the United States and allied forces operating in the Indo-Pacific." Further, it showed that "The PLA is stepping up investment in information operations and adaptive radar systems to jam and blind U.S. sensor and information networks, which PLA leaders judge to be particularly vulnerable."[7] "The PLA is also prioritizing the development of autonomous vehicles, specifically sub-surface and aerial platforms, that suggests it could confer an asymmetric advantage for the PLA in combat with the U.S. or similarly advanced opponent," according to the Center for Security and Emerging Technology at Georgetown University.[8]

From a purely technological standpoint, China has already surpassed the U.S. in computer vision and is a fast follower on Large Language Models (LLMs). In 2022, an aerial imagery object detection global challenge was conducted and the results speak for themselves– the first, second, fourth, and fifth place winners were all Chinese companies or universities.[9]

To close the gap, China is heavily investing and bringing the power of its domestic industrial AI base to support government-backed programs.[10] Since 2020, China has launched 79 LLMs[11] and there are frequent announcements about new national labs opening and state-backed AI companies being formed.[12] The reason for this investment is that "in the AI race between China and the U.S., AI research will be pivotal for China's future success – and hence too important to leave in private hands...State-sponsored AI research is China's Apollo Program."[13]

Scale's Commitment to U.S. National Security

As a patriotic American, I recognized the potential value of Scale's technology for national security use cases and committed to support the United States in preventing President Xi's vision from becoming a reality. For the past three years, Scale has proudly partnered with the U.S. Department of Defense–and stakeholders across the national security space–to integrate our best-in-class

---

[6] See, https://cset.georgetown.edu/publication/harnessed-lightning/

[7] iBid.

[8] See, https://www.army-technology.com/analysis/the-role-of-ai-in-the-peoples-liberation-army/

[9] COCO is the internationally recognized benchmark for image recognition. The leader board can be found here: https://paperswithcode.com/sota/object-detection-on-coco

[10] See, https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf

[11] See, https://www.reuters.com/technology/chinese-organisations-launched-79-ai-large-language-models-since-2020-report-2023-05-30/

[12] See, https://thebambooworks.com/china-goes-it-alone-in-ai-2-0-drawing-on-local-funds-and-trio-of-industry-veterans/

[13] See, https://thediplomat.com/2023/03/the-future-of-state-sponsored-ai-research-in-china/

commercial AI technologies into critical programs that directly impact our national defense. Scale has top American AI talent[14] working on our programs and is actively investing in and committed to teaching and training a homegrown workforce of the future.[15] Our goal is to accelerate AI overmatch for defense and ensure the United States maintains its strategic advantage. This includes:

- ***Scale Autonomous Mission Systems:*** This year, the Defense Innovation Unit (DIU) selected Scale for a critical Army Program Executive Office for Ground Combat Systems (PEO GCS) autonomy. Scale has developed a data engine that is intended to support the Army's Robotic Combat Vehicle (RCV) and that data engine could power any Army autonomous system to enable a new generation of ground vehicles. This critical work has the potential to define the future of the military's work for ground, air, sea, and space autonomy.
- ***Scale Data Engine:*** Scale is working across government agencies to annotate and prepare vast troves of data into a high-quality resource that can be used to train AI models. This is laying the groundwork for AI Overmatch by creating a common data resource. For the U.S. Air Force Research Lab (AFRL), Scale builds and deploys advanced object detection and classification models onto secure networks and integrates those models with existing platforms such as the Air Force Distributed Common Ground System (AF DCGS) to give Airmen access to new AI capabilities within their existing workflows.
- ***Scale Donovan:*** In May 2023, Scale launched Donovan, our AI-powered decision-making platform, which is the first LLM deployed on Department of Defense classified networks. Donovan has the ability to ingest vast amounts of structured and unstructured data to make sense of any aspect of the real world in minutes using simple, natural language. Because it is compatible with the government's own data, end users could share these findings with other trusted networks. For example, a Naval officer could share their findings with intelligence analysts, who then use Donovan to explore a myriad of unstructured documents and quickly detect patterns and trends that would otherwise take weeks to verify and contextualize.

The Era of AI–Data is the Ammunition in AI Warfare

I firmly believe that the United States can still win the race for global AI supremacy, but for the U.S. to maintain this leadership, we must first understand how the landscape is changing and critically examine the DoD's current

[14] See, Forty-two percent of Scale's federal workforce comprises veterans based on self-reported data.
[15]See, https://www.businesswire.com/news/home/20220803005682/en/Scale-Announces-New-Office-in-Downtown-St.-Louis-to-Support-Local-Economic-Growth-and-Tech-Industry-Expansion

capabilities. AI-powered warfare will feature algorithm-fueled military planning, targeting, command and control, and autonomous platforms.[16]

Today, the United States and our allies are confronted with a very real challenge: legacy military platforms are being disrupted by AI. Those platforms, while still important, will be disrupted by cheaper autonomous drone fleets. For example, China has begun testing adaptive drone swarms,[17] which, if used in combat, would turn our legacy aircraft carriers into giant targets.[18]

In the intelligence realm, AI is already playing a critical role because AI applied to satellite imagery and other sensor data has enabled Ukrainian targeting and tracking of Russian troops.[19]

During the daily battle rhythm, the DoD creates more than 22 terabytes of data daily,[20] and because of their outdated data retention and management policies, warfighters, analysts, and operators are unable to tap into its full potential because it is not AI-ready. These potential insights are wasted. The Director of the National Geospatial Intelligence Agency publicly estimated that at the current, accelerating pace of collection, we would need over 8 million imagery analysts by 2027 to process all imagery data.[21] Without AI-ready data, there will be no way to keep pace with our adversaries.

DoD has been working for more than a decade[22] to solve these complex challenges. However, more needs to be done. Early on, and much like other emerging technologies, individual DoD units and end users began learning how to integrate AI into their operations. The DoD has recognized the limiting nature of this approach and the need for a unified strategy. As Deputy Secretary of Defense Kathleen H. Hicks said, "Artificial intelligence may transform many aspects of the human condition, nowhere more than in the military sphere."[23]

One notable step forward took place in May 2021 when Hicks released a memorandum kicking off the creation of the CDAO.[24] The CDAO is critical to

---

[16] See, https://www.amazon.com/Warbot-Dawn-Artificially-Intelligent-Conflict/dp/0197611699
[17] See, https://www.thedrive.com/the-war-zone/37062/china-conducts-test-of-massive-suicide-drone-swarm-launched-from-a-box-on-a-truck
[18] See, https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy
[19] See, https://www.washingtonpost.com/national-security/2022/05/11/ukraine-us-intelligence-sharing-war/
[20] See, https://www.defensenews.com/pentagon/2017/04/06/pentagon-tech-advisers-target-how-the-military-digests-data/"
[21] See, https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf
[22] See, https://www.politico.com/news/magazine/2023/06/15/pentagon-artificial-intelligence-china-00101751
[23] See, https://www.politico.com/news/magazine/2023/06/15/pentagon-artificial-intelligence-china-00101751
[24] See, https://media.defense.gov/2021/May/10/2002638551/-1/-1/0/DEPUTY-SECRETARY-OF-DEFENSE-MEMORANDUM.PDF

ensure a coordinated effort to both the DoD's AI work and its approach to data retention and management.

While this progress is promising, more must be done to achieve AI overmatch.

AI always boils down to data. All of the advancements in commercial AI technologies, such as ChatGPT, have come from using mass troves of data. For this reason, the DoD's own data strategy highlights the importance of prioritizing AI-ready data that is labeled, tagged, and annotated. Additionally, CDAO has the legislative mandate to establish a centralized data repository that will enable the DoD to leverage the power of its own data for AI overmatch. However, implementing this has been challenging because DoD lacks the proper data retention and management systems to operationalize it. Within the DoD, much of our key AI asset—our data—is being wasted every day. This concept is critical to enabling AI platforms of all kinds, but it relies on AI-ready data to succeed, and one of our most critical AI resources is not being used.

China understands this fact. According to an emerging technology expert at the Brookings Institution, "China is renowned for its data collection and thus algorithm development, which will likely define its advantage going forward...The U.S. struggles to reach equivalence in this area, so if China's data collection efforts make for a measurable improvement to its algorithms relative to U.S. ingenuity, China could take the lead."[25]

AI Overmatch–The Path to Global Leadership

To counter this growing threat and win the AI race, we need to achieve AI Overmatch. Adapting to the inevitable transformation of warfare in the AI era will require a shift in the DoD's approach to achieve data supremacy, investment in new technology, Pathfinder Projects, and personnel training. This can only be done successfully by 1) systematic collaboration among Congress, the DoD and industry and 2) developing a regulatory framework that encourages responsible innovation. Today, I would like to propose a five-part framework for achieving it. These pillars represent top-down and bottom-up shifts that should be considered to maintain the U.S.'s security and technological edge:

Investment: China is projected to continue to outpace American investment in AI. Unless we start to prioritize investment in both AI systems and the underlying data infrastructure to power it, we risk falling behind China and doing too little too late.

- While it is important to recognize that more must be done, Scale was pleased to see the FY24 President's budget request that recommends $1.8

[25] See, https://www.japantimes.co.jp/news/2023/04/20/asia-pacific/china-ai-future-wars/

billion in DoD AI investment.[26] It is critical that this funding is upheld through conference as another 12 months is too long to wait to adequately fund AI development.

Data Supremacy: AI systems are only as good as the data that they are trained on, and leading the world in developing AI-ready data is an absolute requirement to maintain our strategic advantage in the era of AI warfare. The advancements in LLMs over the past 5 years, including ChatGPT, have been achieved through training models on 1000 times more data than previously done. We must aim to accomplish a similar 1000 fold increase in our DoD AI implementations.

- Scale has been pleased to see Congress prioritize the CDAO and its legislative mandate to create a centralized data repository. It is critical that Congress continues to heavily invest in AI-ready data.

Test and Evaluation: One of the most important ways to ensure that AI models provide reliability and accountability for users is through a risk-based approach to test and evaluation with human oversight. We believe that this not only protects taxpayer resources by ensuring that Congress acquires high-quality AI systems, but also is one of the strongest methods to limit bias and uphold the DoD Ethical AI Principles.[27]

- Test and evaluation has long been a key part of the product development cycle for responsibly bringing consumer-facing technologies to market and military technologies into production. This is essential for AI applications because they are rapidly developing and constantly iterating, and therefore continually presenting new opportunities and risks to the end user.
- A risk-based approach to test and evaluation will ensure that AI is factual, accurate, and explainable regardless of the underlying model or data being used. If the product–including the data infrastructure and underlying model–does not meet these requirements, we risk sacrificing user trust in the technology.
    - The Biden Administration has embraced this concept by highlighting Scale's role building an evaluation platform for existing LLMs at the world's leading hacker conference, DEFCON, in August.[28] Scale recommends that Congress adopts comprehensive, risk-based test and evaluation criteria to ensure that AI will meet user safety and reliability standards prior to deployment within the DoD.

---

[26]See, https://www.defense.gov/News/Releases/Release/Article/3326875/department-of-defense-releases-the-presidents-fiscal-year-2024-defense-budget/

[27] See, https://www.ai.mil/blog_02_26_21-ai_ethics_principles-highlighting_the_progress_and_future_of_responsible_ai.html#:~:text=These%20principles%20encompass%20five%20areas,lifecycle%20both%20interactively%20and%20iteratively.

[28] See, The White House, Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans' Rights and Safety, Washington DC, May 04, 2023

Pathfinder Projects: Congress and DoD need to commit to supporting new AI Pathfinder Projects–projects that have the mission and funding to solve unique DoD challenges.

- To date, the largest AI Pathfinder Project within DoD is still Project Maven, which began in 2017. In the past six years, there have been many important lessons learned, but no new efforts have been initiated.
    - There are endless DoD use cases that would benefit from being identified as a Pathfinder Project. For example, the Army is making progress on Project Linchpin and their ground autonomy work; Joint All Domain Command and Control (JADC2) requires DoD buy-in at all levels to succeed; and the Navy has discussed a concept called Project Overmatch, which would create a whole-of-Navy approach to AI adoption. While much work is being done to define these projects, Scale recommends that Congress pushes each branch of the military to formally identify its next Pathfinder Project and adequately fund it to be successful.

Personnel Training: The U.S. should invest in rapidly training and upskilling our military commanders and personnel on AI.

- Even with advancements in technology, humans always pay the price of war. The U.S should continue to invest heavily to ensure that its military has the best equipment, training, and leadership in the world, and part of the necessary training to succeed in the next era of warfare will be advanced AI literacy across all military units. This is crucial as we fully embrace the era of AI.
- Beyond simply training service members on AI fundamentals, the US should train commanders and personnel with necessary data skill sets to adopt AI in a way that will make multi-domain warfare a reality.
- Scale has the experience to understand this challenge and lend our expertise in a way that benefits the United States and economy broadly. We established a hub in St. Louis, which has created more than 300 tech-focused jobs, which range from entry-level labelers to machine learning engineers with advanced degrees. We anticipate growing these opportunities in the future. Scale looks forward to working with Congress and the DoD to identify technical gaps in current skill sets and how to best address those gaps.

Conclusion

The race for global AI leadership is well underway, and I could not be more excited to do everything in my power to ensure that the U.S. wins. This is one of the few true missions of our time that will define the future of war and global politics. We cannot sit by the sidelines, and it is in moments like this that

Congress, the DoD, and the tech industry can either rise to the challenge together or stand idle.

I am filled with a sense of optimism as we stand on the cusp of a new era, where these challenges are being met head-on by brilliant leaders across the public and private sectors. I am honored to work with this subcommittee to forge strong relationships between Congress, DoD, and the tech industry so we can collaborate and stay ahead of some of the most pressing threats of the next decade.

Thank you for the opportunity to be here today. I look forward to your questions.

Alexandr Wang
Chief Executive Officer, Scale AI

Alexandr Wang is the founder and CEO of Scale AI, the data platform accelerating the development of artificial intelligence. Alex founded Scale as a student at MIT at the age of 19 to help companies build long-term AI strategies with the right data and infrastructure.

His technical expertise, combined with a laser focus on data quality and accuracy, has led Scale to rise above the competition and meet the demand for intelligent software. Scale is currently valued at $7.3 billion and provides AI solutions tailored to business use cases and machine learning tools to unlock breakthroughs like Generative AI and operationalize AI for all organizations spanning the U.S. government, researchers, startups and Fortune 500 companies across e-commerce, logistics, technology, fintech, and more industries. Organizations such as Meta, Microsoft, Open AI, General Motors, SAP, Flexport and the U.S. Army partner with Scale to solve problems with data labeling and annotation, scenario-based model testing and validation, content understanding and contextualization, AI catalog for asset reusability and more.

Alex believes high-quality data, with the right tools and infrastructure, will enable enterprises to deploy AI as easily as they deploy code. Scale is an AI readiness partner, helping teams manage the entire ML lifecycle, from data annotation and curation to model testing and evaluation, enabling any organization – from the world's most advanced AI teams to legacy organizations – to develop and deploy impactful AI solutions. Scale combines ML technology with skilled human insight to ensure every AI application is built on a foundation of high-quality ground truth data.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 118th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: 7/18/2023

Hearing Subject:

Machine Learning and Human Warfare: Artificial Intelligence on the Battlefield

Witness name: Alexandr Wang

Position/Title: Founder & CEO

Capacity in which appearing: (check one)

○ Individual ◉ Representative

If appearing in a representative capacity, name of the organization or entity represented:

Scale AI, Inc.

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2023

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
OT Agreement	ARMY	$355,000.00	Ground Autonomy Data Infra
Subagreement	CDAO	$605,000.00	LLM Testing and Support
OT Agreement	CDAO	$6,900,000.00	Data Annotation
CRADA	DoD	$0	AI Model Development & Testing

2022

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Contract	USAF	$945,000.00	Smart Infrastructure R&D
Contract	USAF	$1,000,000.00	Smart Infrastructure R&D
OT Agreement	DIU	$1,541,167.00	Autonomous Perimeter Security
Subcontract	AFRL	$1,811,400.00	AI Model Development & Testing
Subcontract	NGA	$3,200,000.00	Data Annotation Infra

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Contract	AFRL	$749,942.00	ISR CV Model Development
Subcontract	DIU	$75,000.00	Data Annotation
Subcontract	NGA	$250,000.00	AI Assisted Damage Assessments

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Contract	ARMY	$106,713,949.19	AI Data Infra and Annotation R&D
Subcontract	ARMY	$3,328,211.85	Data Annotation

Foreign Government Contract, Grant, or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2023

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2022

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2023

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Purchase Order	Booz Allen Hamilton	$300,000.00	LLM Testing and Support

2022

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Purchase Order	Lockheed Martin	$294,999.98	Data Annotation
Purchase Order	Lockheed Martin	$900,000.00	Data Annotation
Purchase Order	Booz Allen Hamilton	$40,000.00	Data Annotation
Purchase Order	Booz Allen Hamilton	$75,000.00	Data Annotation

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Purchase Order	Lockheed Martin	$249,999.00	Data Annotation

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Purchase Order	Palantir	$250,000.00	Data Annotation

AMERICAN ENTERPRISE INSTITUTE

Statement before the House Committee on Armed Services
Subcommittee on Cyber, Information Technologies, and Innovation
On *Man and Machine: Artificial Intelligence on the Battlefield.*

AI Is a National Security Lifeline

Klon Kitchen
Senior Fellow

July 18, 2023

Opening Statement

Good morning, Chairman Gallagher, Ranking Member Khanna, and members of the committee. Thank you for the privilege of testifying.

I'd like to use my opening statement to make three points.

First, I believe artificial intelligence (AI), and particularly emerging capabilities like generative AI, are a national security lifeline for the United States. The national security community has discussed the potential of AI for years, but now it seems these technologies are finally maturing to where they can be applied at scale – with few doubting that they will soon reshape almost every part of our lives, including how we fight and win wars.

The importance of AI is felt as acutely in Beijing as it is in Washington, but until recently, I was not at all confident that the United States would hold the AI advantage. If you assume this advantage fundamentally comes down to algorithms, data, and hardware – just one year ago, I would have given the United States the advantage on algorithms, the Chinese the advantage on data, and I would have called hardware a "jump ball" between the two nations because, while the U.S. designs the most advanced semiconductors in the world, they are overwhelming produced deep within China's sphere of influence. But now I'm giving this assessment another look.

Large Language Models and other generative AIs may be moving the competition back to the American advantage. The U.S. continues to dominate the underlying computer science and algorithms giving birth to these advancements and we continue to be the location of choice for the world's most brilliant minds.

On hardware, a strong bipartisan consensus is allowing us to meaningfully constrain China's access to cutting-edge capabilities like advanced graphics processing units (GPUs) and even more can and should be done, for example, limiting Chinese cloud services would be an excellent next step.

Finally, on data, while the Chinese economy and people continue to generate a deluge of digitized data and while the Chinese Communist Party (CCP) continues to have unfettered access to these data, the fact that many of the new AI models are indexed on the open internet may blunt the CCP's advantage. It is my hope, for example, that the Chinese government's political fragility, strict content controls, and general oppression of its own people will compromise or bias much of the data that it collects, diluting its utility and ultimately limiting the development of Chinese AI. At the very least I think the United States has an opportunity to surge ahead of Beijing on AI if we properly seize this moment.

But AI offers the U.S. more than bespoke capabilities, Large Language Models and other generative technologies – if properly realized – could provide an economic base for a new era of American prosperity and security. For years, we have known that the United States is not investing in its military sufficiently to enable it to meet the demands of the nation. The truth of this has been laid bare as our defense industrial base struggles to keep up with the demand of supporting Ukraine's noble fight against Vladimir Putin illegal and evil invasion of that nation. But, according to one recent study, existing GenAI "could add the equivalent of $2.6 trillion to $4.4 trillion annually" to the global economy, and "this estimate would double if we include the impact of embedding generative AI into software that is currently used."[i]

The bottom line is this: I believe AI is offering us an opportunity to get our economic house in order, to lay a foundation for our nation's long-term prosperity, and to build a national security

enterprise that is sufficiently resourced to secure that prosperity for a generation or more.

But finally, while AI offers all this promise and more, it also has some serious national security risks – most acutely a flood of misinformation and disinformation operations and the exponential growth of conventional and novel cyber-attacks.

By now we have all seen the photos, videos, and other media generative AIs are creating and these capabilities have been almost immediately democratized. Virtually anyone, anywhere in the world, can now create and distribute synthetic media that will undoubtedly be used to undermine American confidence in our democratic institutions and free society. Similarly, generative AIs will offer hostile cyber actors potent tools for generating and automating traditional and new online attacks. In a world where we are already overwhelmed by online threats, generative AIs will soon pour gas on these fires.

There is much more that I could say on these matters, but I trust we'll cover them more fully over the course of this hearing. Thank you again for the opportunity to testify and I look forward to your questions.

Background

Artificial Intelligence (AI), particularly generative AI (GenAI), offers a substantial opportunity for the United States to reclaim its technological and economic upper hand on the global stage. By deploying AI power, the U.S. can accelerate innovation, encourage economic growth, and sustain its leadership in the technology sector – all of which facilitate the nation's security interests.

GenAI holds the potential to reshape various industries, including healthcare, finance, manufacturing, and entertainment. Advanced AI models, like OpenAI's GPT, can create realistic text, images, and even music. This paves the way for creative applications, content creation, and personalized user experiences. With GenAI, American companies can craft innovative products and services that meet evolving market demands, which would foster economic growth and create new jobs.

For example, according to a recent McKinsey and Company study, GenAI "could add the equivalent of $2.6 trillion to $4.4 trillion annually" to the global economy, and "this estimate would double if we include the impact of embedding generative AI into software that is currently used."[ii]

AI-driven automation can also boost productivity and efficiency across sectors, enabling American businesses to compete on the global stage. Intelligent automation can enhance operations, optimize supply chains, and improve decision-making processes. This can result in cost savings, increased output, and improved competitiveness for American industries.

Here again, McKinsey's study concludes, "Current generative AI and other technologies have the potential to automate work activities that absorb 60-70 percent of employees' time today." It adds that "…half of today's work activities could be automated between 2030 and 2060, with a midpoint in 2045, or roughly a decade earlier than in our previous estimates."[iii]

The U.S.' potential to reclaim its competitive advantage is evident in the wealth of talent and expertise in the AI field. American universities and research institutions have led AI research, producing pioneering advancements and cultivating a skilled workforce. Furthermore, the U.S.

hosts a dynamic ecosystem of AI startups and technology companies that are driving innovation and attracting global investments. For example, American companies have led breakthroughs in machine learning, computer vision, natural language processing, and other AI disciplines. These advancements have yielded transformative technologies like voice assistants, autonomous vehicles, and personalized recommendations. The U.S. has also led in deploying AI technologies across sectors, including finance, healthcare, and e-commerce, driving significant economic growth.

It is also important to underscore how much American policymakers are united in their understanding of the strategic importance of AI and have actively supported its development. The U.S. government has invested in AI research, encouraged academia-industry collaborations, and promoted the adoption of AI technologies in public sectors. These initiatives reveal a commitment to fostering an AI-driven economy and maintaining American leadership in the global technology landscape.

AI, particularly GenAI, presents a remarkable opportunity for the U.S. to reclaim its technological and economic dominance. By exploiting AI's transformative potential, investing in research and development, and nurturing talent, the U.S. can accelerate innovation, create jobs, and sustain its leadership in the global AI landscape. The country's historical successes, along with its robust AI ecosystem and supportive policies, position it favorably to seize this opportunity and secure its technological and economic future.

This new efficiency and prosperity should be the backbone of a renewed American military and national security enterprise that is resourced to meet our nation's global interests and priorities. But, even if the U.S. does everything right, many of our partners are approaching AI and other technologies in ways that will constrain—or even imperil—our shared security concerns.

Military Interoperability

The U.S. and its allies should pursue complementary approaches to AI and other emerging technologies, considering the private sector's critical role in AI and related technologies.

Indeed, the significant role of the private sector in GenAI development is a key reason for focusing on regulatory interoperability. Private companies are leading AI innovation, investing heavily in research and development. Their expertise and resources centrally position them to shape the trajectory of AI technologies. As the private sector operates globally, regulatory interoperability becomes crucial for effective engagement and collaboration between companies across different countries and, more importantly, for the interoperability of military capabilities.

The ability for allied forces to seamlessly collaborate is essential for joint missions and coalition efforts. Specifically, aligning regulations, standards, and ethical frameworks among allies is crucial to ensure smooth coordination and information sharing.

Military interoperability is particularly important in the context of GenAI. GenAI technologies, with their potential for autonomous decision-making and advanced capabilities, require close coordination and trust among allied forces. By adopting complementary approaches, the U.S. and its allies can establish common guidelines and principles for the development, deployment, and use of GenAI in military applications. This ensures that AI systems adhere to shared ethical norms, respect international humanitarian law, and are compatible with each other, enabling effective joint operations. But some of our allies appear not to understand this.

Regulatory Interoperability

Unfortunately, many of our closest partners, especially in Europe, are pursuing policies that risk stifling innovation and creating barriers to market entry for American companies. The European Union's proposed AI Act, along with other technology regulations targeting American tech companies, are already negatively impacting both the American tech industry and the global technology landscape.

The AI Act introduces strict rules and requirements for AI systems, including "high-risk" applications. While these regulations aim to ensure ethical and responsible AI deployment, the Act's provisions are overly prescriptive and hinder innovation. The compliance costs and regulatory complexities may disproportionately impact smaller tech companies, including startups, limiting their ability to compete and thrive in the European market. And this is broadly recognized even among European technology companies.

For example, recently more than 150 European companies issued a public letter criticizing the AI Act, arguing that the EU's heavy-handed approach is threatening EU digital sovereignty and calling for active industry involvement from companies on both sides of the Atlantic. "Such regulation," the letter warns, "cold lead to highly innovative companies moving their activities abroad, investors withdrawing their capital from the development of the European Foundation Models and European AI in general."[iv] But this is not the only challenge.

The EU's focus on data localization and data sovereignty further exacerbates the potential negative impact on American tech companies. The proposed regulations aimed at promoting the storage and processing of data within the EU would limit the ability for American tech companies to efficiently operate and deliver services in the European market. These regulations not only create an uneven playing field that may favor domestic European competitors, but it also disrupts the seamless exchange of data needed to address common global challenges, such as privacy, cybersecurity, and the responsible deployment of AI.

Adopting complementary approaches to AI and emerging technologies allows the US and its allies to leverage their collective strengths. Each country brings unique expertise, resources, and perspectives to the table. By working together, they can share best practices, collaborate on research and development, and jointly tackle common challenges.

Beyond helping our friends assume a more productive posture on AI and emerging technologies, the U.S. should also prepare for how our adversaries might seek to use these capabilities to subvert the American people and our national interests.

Foreign AI Threats

The rapid advancement of GenAI poses a significant near-term threat concerning its potential use against us by foreign adversaries. One of the most concerning aspects is the exponential growth of traditional cyber threats in both speed and scale. The convergence of GenAI and cyberattacks magnifies the potential risks and challenges faced by nations, governments, and individuals in defending against these threats.

Foreign adversaries leveraging GenAI can significantly increase the speed at which cyberattacks are executed. AI-powered systems can autonomously scan and exploit vulnerabilities in

computer networks and software at an unprecedented pace. This acceleration allows adversaries to infiltrate systems rapidly, extract sensitive information, or disrupt critical infrastructure. With the ability to quickly automate and execute attacks, the response time for defenders becomes increasingly limited, amplifying the potential damage caused by cyberattacks.

The scalability of GenAI-driven cyber threats is another alarming aspect. Adversaries can utilize AI-powered bots and algorithms to orchestrate large-scale attacks, overwhelming networks and systems. Distributed denial-of-service (DDoS) attacks, for example, can be amplified through AI-controlled botnets, causing severe disruptions to online services and critical infrastructure. The ability to orchestrate simultaneous attacks on multiple targets with minimal human intervention increases the potential for large-scale cyber disruptions and undermines the stability of nations and economies.

Moreover, GenAI enhances the sophistication and effectiveness of cyber threats. AI algorithms can learn and adapt to defensive measures, making attacks more evasive and difficult to detect. Adversaries can leverage AI's ability to analyze vast amounts of data to identify patterns, exploit weaknesses, and craft customized attacks. By constantly learning and evolving, GenAI-powered cyberattacks become more sophisticated, resilient, and capable of bypassing traditional security measures.

Finally, there is also the potential for foreign adversaries to leverage GenAI for social engineering and psychological manipulation. AI algorithms can analyze and understand human behavior patterns, preferences, and vulnerabilities, enabling adversaries to tailor attacks with precision. By leveraging this technology, adversaries can craft convincing phishing emails, generate realistic deep fake videos, or manipulate public opinion through targeted disinformation campaigns. The combination of GenAI's computational power and psychological insights can exponentially amplify the impact of such attacks, posing significant risks to national security and social cohesion.

To address this near-term threat, it is essential for governments, cybersecurity experts, and technology companies to collaboratively develop robust defenses against GenAI-powered cyber threats. This includes leveraging AI and machine learning technologies to enhance threat detection, automate responses, and mitigate the risks posed by AI-driven attacks.

International cooperation is also crucial in establishing norms, agreements, and frameworks to address the malicious use of AI technologies. Encouraging information sharing, promoting transparency, and establishing guidelines for responsible AI development can help mitigate the risks posed by foreign adversaries. Additionally, fostering public-private partnerships is vital to exchange knowledge, resources, and best practices in addressing the evolving cyber threat landscape. But there are other near-term threats beyond traditional cybersecurity.

The arrival of GenAI also introduces the potential for low-friction misinformation and disinformation operations that pose significant challenges to democratic institutions in the U.S. Specifically, GenAI's ability to rapidly generate and disseminate vast amounts of convincing content can amplify the spread of misinformation, degrade trust in institutions, and undermine democratic processes reliant on informed decision-making and an educated citizenry.

One of the key implications of GenAI-enabled misinformation and disinformation operations is the speed and scale at which false or misleading information can be generated and disseminated. AI algorithms can swiftly produce and distribute content that appears legitimate, making it

increasingly difficult for users to distinguish between real and fake information. This allows malicious actors to manipulate public opinion, exploit existing biases, and intensify societal divisions with minimal effort and cost.

Moreover, GenAI can generate highly personalized and targeted content, designed to exploit individuals' vulnerabilities and preferences. By analyzing vast amounts of data, AI algorithms can understand users' interests, beliefs, and behaviors, enabling the creation of hyper-targeted misinformation campaigns. This level of personalization enhances the persuasive power of disinformation, making it more likely for individuals to be influenced and reinforce echo chambers that undermine public discourse.

Furthermore, GenAI-powered disinformation campaigns can influence electoral processes, threatening the integrity of democratic elections. Malicious actors can leverage AI algorithms to amplify divisive narratives, suppress voter turnout, or manipulate public opinion to favor specific candidates or causes. The proliferation of misinformation can create an environment where the truth becomes obscured, and electoral outcomes are skewed, compromising the legitimacy and fairness of democratic processes.

Ultimately, the widespread dissemination of misinformation and disinformation erodes trust in democratic institutions. When false or misleading information proliferates unchecked, public trust in media, government, and other authoritative sources can diminish. This undermines the foundation of democratic societies, as citizens rely on accurate information to make informed decisions, hold elected officials accountable, and engage in meaningful political discourse.

Addressing the challenges posed by GenAI-enabled misinformation and disinformation requires a multi-faceted approach. It involves collaboration among governments, technology companies, civil society, and the public. Efforts should focus on developing robust fact-checking mechanisms, promoting media literacy, and improving digital literacy among citizens. Technology companies should enhance their algorithms and platforms to detect and counteract the spread of false information. Governments can play a role by implementing legislation that promotes transparency, accountability, and the responsible use of AI technologies.

While cybersecurity and misinformation and disinformation will be critical near-term challenges, advancing AI will also provoke more systemic and strategic challenges for national security leaders over the long-term. Specifically, we will need to navigate the unprecedented level of knowledge AI can provide, the opacity of AI decision-making processes, the authority granted to AI systems, and the potential for lethal autonomy.

Long-Term Challenges of AI

As aforementioned, one of the premiere challenges of AI is its acquisition of knowledge at an unprecedented scale and speed. AI algorithms can process vast amounts of data, analyze patterns, and derive insights that surpass human capabilities. This knowledge can be immensely valuable for a range of applications, from scientific discoveries to business insights. However, as we accumulate more knowledge, it becomes increasingly challenging to manage and interpret this information effectively. The sheer volume and complexity of AI-generated knowledge require careful navigation and the development of robust frameworks for verification, validation, and interpretation.

The second challenge arises from the opacity of AI decision-making processes. As AI systems

become more sophisticated, they employ complex algorithms that can yield accurate results but may not provide explainable or interpretable rationales. In certain cases, AI can produce correct outcomes without us fully understanding how it arrived at those conclusions. This lack of explainability can be problematic, especially in critical domains where transparency and accountability are essential. It raises concerns about biases, ethical implications, and the potential for unintended consequences. Striking a balance between the accuracy and explainability of AI systems is an ongoing challenge that requires careful consideration and research.

The third challenge is related to the authority granted to AI systems. As AI algorithms demonstrate impressive performance and accuracy, there is a tendency to rely heavily on their decisions and recommendations. However, AI systems are not infallible and can make errors or encounter scenarios outside their training data. The challenge lies in discerning when AI is authoritative and when human judgment should prevail. It requires understanding the limitations of AI systems, designing appropriate checks and balances, and establishing clear boundaries for human oversight and intervention. Striking the right balance between human judgment and AI authority is crucial to ensure responsible and accountable decision-making.

The fourth, and perhaps most contentious challenge, is the emergence of lethal autonomy. Lethal autonomous systems refer to AI-powered machines or weapons that can independently identify and engage targets without direct human control. The development of such systems raises ethical and legal questions, as it has the potential to be abused or create unintended consequences. The challenge lies in determining the appropriate policies, regulations, and safeguards to ensure that lethal autonomous systems adhere to international humanitarian law, ethical principles, and the principles of proportionality and distinction in armed conflict. It requires international cooperation, robust ethical frameworks, and clear guidelines to prevent the escalation of conflicts or the loss of human control over life-and-death decisions.

Addressing these challenges requires a comprehensive and multidisciplinary approach. It involves collaboration among policymakers, researchers, industry leaders, and civil society to develop ethical guidelines, regulatory frameworks, and technical solutions. Transparency and accountability in AI systems are paramount, necessitating efforts to enhance explainability and interpretability. Ongoing research in AI ethics, fairness, and bias mitigation is crucial to ensure that AI is deployed responsibly and does not perpetuate or amplify existing societal inequities.

Moreover, as has been reiterated throughout my testimony, international cooperation is essential in addressing the challenges posed by AI technologies. Establishing global norms and agreements can help guide the development, deployment, and use of AI in a manner that respects human rights, privacy, and security. It can also promote cooperation in areas such as data sharing, research collaboration, and the prevention of malicious uses of AI.

In conclusion, as AI continues to advance, there are inherent challenges that we need to navigate. These challenges include managing an unprecedented level of knowledge, addressing the opacity of AI decision-making processes, determining the appropriate balance between AI authority and human judgment, and grappling with the potential implications of lethal autonomy. Addressing these challenges requires multidisciplinary collaboration, transparency, accountability, and ongoing research and innovation. By proactively tackling these challenges, we can harness the potential of AI while ensuring its responsible and beneficial integration into our society.

Again, I thank the committee for the opportunity to share these observations and I look forward to your questions.

[i] McKinsey and Company. *The economic potential of generative AI: The next productivity frontier.* 14 June 2023.<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of generative-ai-the-next-productivity-frontier#introduction>.

[ii] McKinsey and Company. *The economic potential of generative AI: The next productivity frontier.* 14 June 2023.<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of generative-ai-the-next-productivity-frontier#introduction>.

[iii] Ibid.

[iv] Butcher, Mike. *European VCs and tech firms sign open letter warning against over-regulation of AI in draft EU laws*. 30 June 2023.<https://techcrunch.com/2023/06/30/european-vcs-tech-firms-sign-open-letter-warning-against-over-regulation-of-ai-in-draft-eu-laws/>.

Klon Kitchen
Nonresident Senior Fellow
American Enterprise Institute

Klon Kitchen is a nonresident senior fellow at the American Enterprise Institute (AEI), where he focuses on the intersection of national security and defense technologies and innovation. Through his research, he works to understand and explain how emerging technologies are shaping modern statecraft, intelligence, and warfighting, while focusing on cybersecurity, artificial intelligence, robotics, and quantum sciences.

Before joining AEI, Mr. Kitchen was director of the Heritage Foundation's Center for Technology Policy, where he led an enterprise-wide, interdisciplinary effort to understand and shape the nation's most important technology issues.

Before joining Heritage, Mr. Kitchen was national security adviser to Sen. Ben Sasse (R-NE) and worked on the creation of the US Cyberspace Solarium Commission, a blue-ribbon commission tasked with developing an American grand strategy for cyber. While working for Sen. Sasse, Mr. Kitchen served as the staff director of the National Security and International Trade and Finance Subcommittee for the Senate Committee on Banking, Housing, and Urban Affairs.

Mr. Kitchen has also worked on cyber strategy at the National Counterterrorism Center; as a senior program assessment officer at the Office of the Director of National Intelligence in the Office of the Director of Central Intelligence; and as the lead analyst on al Qaeda senior leadership at the Defense Intelligence Agency. He was also the National Counterterrorism Center chair at National Defense University.

A popular speaker, Mr. Kitchen has appeared on "60 Minutes" on CBS News and The New York Times podcast "The Argument." He has also been published in RealClearDefense, The Hill, The National Interest, The Telegraph, Washington Examiner, and National Affairs, among other outlets.

Mr. Kitchen has an MA in strategy and security studies from the College of International Security Affairs and a War College Diploma in security strategy and irregular warfare from the National War College, both from National Defense University. His BA in biblical studies is from Bryan College.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 118th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: 7/18/2023

Hearing Subject:

Machine Learning and Human Warfare: Artificial Intelligence on the Battlefield

Witness name: Klon Kitchen

Position/Title: Non-resident Senior Fellow, American Enterprise Institute

Capacity in which appearing: (check one)

● Individual ○ Representative

If appearing in a representative capacity, name of the organization or entity represented:

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2023

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
NA	NA	NA	NA

2022

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
NA	NA	NA	NA

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
NA	NA	NA	NA

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
NA	NA	NA	NA

Foreign Government Contract, Grant, or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2023

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
NA	NA	NA	NA

2022

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
NA	NA	NA	NA

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
NA	NA	NA	NA

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
NA	NA	NA	NA

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship
NA	NA

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2023

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
NA	NA	NA	NA

2022

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
NA	NA	NA	NA

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
NA	NA	NA	NA

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
NA	NA	NA	NA

Testimony of Haniyeh Mahmoudian, Global AI Ethicist

Before the

U.S. House Armed and Services Committee

Subcommittee on Cyber, Information Technologies, and Innovation

Hearing on "Machine Learning and Human Warfare: Artificial Intelligence on the Battlefield"

Tuesday, July 18, 2023

Chair Gallagher, Ranking member Khanna, and the distinguished members of the Cyber, Information Technologies, and Innovation subcommittee:

Thank you for the opportunity to testify before the subcommittee on the critical issue of Machine Learning and Human Warfare: Artificial Intelligence on the Battlefield. My name is Dr. Haniyeh Mahmoudian, and I am an AI Ethicist. In my individual capacity, I am an advisory member of the National Artificial Intelligence Advisory Committee (NAIAC) and co-chair the AI future Working Group. I am currently employed as a Global AI ethicist at DataRobot. I am testifying today in my individual capacity and not on behalf of any entity or organization. My testimony and views I express today are my own and should not be contributed to any other organization, entity, or individuals.

My background is in machine learning and artificial intelligence (AI) and in the past five years, my focus has been on AI bias and more broadly responsible AI. In my capacity as a Global AI Ethicist at DataRobot, in addition to providing educational support on AI ethics, I have worked with engineering and product teams to incorporate principles of trustworthy AI into the product. The importance of incorporation of AI ethics and responsible AI frameworks in AI utilized in warfare cannot be overstated. Therefore, I am grateful for the committee's attention to AI governance and responsible use of AI in the military and for inviting me to share my insights and expertise.

Importance of AI

AI holds immense potential and is poised to revolutionize nearly every facet of our lives, from how we work, communicate, to how we solve complex problems. It's a field that has grown exponentially in recent years, underpinned by advances in computational power, data availability, and innovations in machine learning algorithms..

AI is increasingly becoming an essential component of modern military strategies and operations, holding the potential to revolutionize how nations prepare for and conduct military missions. AI's influence is seen across a broad spectrum of military applications, each profoundly impacting operational efficiency and decision-making.

In the realm of cybersecurity, AI can help protect military networks and systems against increasingly sophisticated cyber threats. By continually learning from new data, AI can identify and respond to novel cyber-attacks more effectively than traditional systems. Furthermore, AI can assist in offensive cybersecurity operations, identifying vulnerabilities in enemy networks and systems.

AI's role in predictive maintenance is another noteworthy application. By analyzing data from military equipment, AI can predict when parts might fail and recommend proactive

maintenance, improving the reliability and readiness of military hardware. This can lead to cost savings and increased operational efficiency by minimizing unplanned downtime and preventing catastrophic failures.

AI also plays a crucial role in injury prediction and prevention among military personnel. Using data gathered from sensors worn by soldiers and machine learning algorithms, AI can effectively track real-time physical fatigue and potential injuries. This could aid in prevention of musculoskeletal injuries (MSK) and other bodily injuries. According to the U.S. Army Public Health Center, musculoskeletal injuries among active-duty soldiers result in over 10 million restricted-duty days each year, and constitute more than 70% of the medically non-deployable population. These types of injuries, along with their subsequent impacts, are a major reason for medical disability and consequent discharge from service.[1]

Text analysis is another area where AI can rapidly review and analyze intelligence reports, swiftly translating or decoding local or coded languages. It can detect trends, specific words, or phrases and extract key information rapidly. AI's ability to process and analyze vast amounts of data from various sources surpasses human capacity. It helps identify patterns, detect real-time threats, and highlight only the most relevant information, enhancing the speed and effectiveness of military decision-making.

It is imperative that the United States expedite the adoption of AI to sustain our strategic advantage, especially in the military. While these benefits are significant, it is crucial to ensure that the use of AI in military contexts adheres to legal and ethical guidelines, particularly regarding decision-making in lethal operations. As AI continues to evolve, it will undoubtedly play a more prominent role in shaping the future of military strategy and operations.

Why Ethical and Responsible AI Matter

As technology has advanced, the ethical and moral considerations of its application have always been a topic of discussion. These concerns have intensified due to the swift progress in AI, its widespread adoption, and larger impact on our lives. In recent years, insufficient scrutiny and evaluation of AI systems, coupled with a limited comprehension of AI's potential adverse effects, have led to numerous instances where AI, despite being developed with noble intentions, ended up harming the vulnerable individuals and communities it was designed to help or inadvertently discriminated against marginalized groups. This suggests that considerations of AI Ethics have often been relegated to a secondary concern when building and deploying AI systems.

---

[1] https://militaryembedded.com/ai/machine-learning/using-sensors-and-ml-to-prevent-warfighter-injury

To fully leverage the power of AI, particularly in governmental applications such as the military, it's crucial to garner public trust by ensuring AI is effective, reliable, and ethically built and operated. This necessitates the establishment of ethical and responsible AI frameworks for the creation and implementation of AI systems. Such measures should protect civil liberties and rights, guarantee fairness, and instate a robust AI governance system with accountability at its core.

It is encouraging that the Department of Defense has taken initiatives to develop AI ethics principles that will apply to both combat and non-combat functions and assist the U.S. military in upholding legal, ethical, and policy commitments in the field of AI. As former Secretary Esper has remarked, "AI technology will change much about the battlefield of the future, but nothing will change America's steadfast commitment to responsible and lawful behavior. The adoption of AI ethical principles will enhance the department's commitment to upholding the highest ethical standards as outlined in the DOD AI Strategy, while embracing the U.S. military's strong history of applying rigorous testing and fielding standards for technology innovations"[2].

Building Trust into AI

Responsible AI encompasses the ethical approach to designing, building, and deploying AI systems. Its aim is to utilize AI in a manner that prioritizes safety, trustworthiness, transparency, and more broadly ethical considerations. Embracing responsible AI practices promotes transparency and addresses concerns related to AI bias, thereby ensuring a more equitable and reliable application of AI technology.

Implementing responsible AI frameworks and fostering trust in AI systems requires consideration of people, processes, and technology. Various stakeholders participate in the AI lifecycle. It is crucial that individuals involved in the process of building, deploying, and using AI systems have AI literacy. The AI Initiative Act of 2020 (NAIIA) instructs the President, via the National AI Initiative Office, to continually uphold AI research and development. This includes promoting AI education and worker training schemes, endorsing interdisciplinary AI study and educational programs, and arranging and coordinating Federal interagency AI efforts[3]. "The National AI Initiative Act calls for agencies to prioritize fellowship and training programs to help American workers gain AI-relevant skills through skills programs, fellowships, and education in computer science and other growing Science, Technology, Engineering, and Math (STEM) fields"[4]. In Addition, to ensure the responsible use of AI, stakeholders should be provided with educational resources relevant to their roles and responsibilities on AI ethics and

[2] DOD Adopts Ethical Principles for Artificial Intelligence > U.S. Department of Defense > Release
[3] ABOUT - National Artificial Intelligence Initiative (ai.gov)
[4] EDUCATION AND TRAINING - National Artificial Intelligence Initiative

practical approach to apply the Department of Defense's AI ethics principles in their workflow and use cases.

AI governance refers to the system of rules, policies, and procedures designed to manage and oversee the development, deployment, and ongoing use of AI technologies. It's an approach to regulate the lifecycle of AI, which includes stages such as data collection and processing, model development, training and testing, deployment, and continuous monitoring. Implementing an AI governance framework and standardizing the AI lifecycle can help agencies work more effectively, and to proactively address the concerns inherent in their operations. AI governance is critical for several reasons. It establishes a structure for ethical AI use, ensuring that the development and application of AI technologies are aligned with societal values and norms, manages risk, and mitigates potential harm. AI can have unintended consequences, and strong governance can provide processes to evaluate, monitor, and mitigate these risks. In this regard, the National Institute of Standards and Technology (NIST) has made notable contributions by developing AI risk management frameworks and has recently released its AI Risk Management Framework 1.0[5]. In its first report, the National AI Advisory Committee (NAIAC) recommends that the White House encourage Federal agencies to implement NIST or similar processes to address risks associated with AI in its lifecycle with appropriate evaluations and monitoring[6]. In addition, governance ensures compliance with laws and regulations and promotes accountability and transparency. It ensures there are clear lines of responsibility for AI systems and their outcomes, and that these systems and their decision-making processes are transparent and explainable. In essence, AI governance can serve as a roadmap for the Department of Defense, guiding them on how to responsibly develop and use AI while managing risks and ensuring public trust. As the use of AI grows and evolves, the importance of robust AI governance will only continue to increase.

Human-centered design is a crucial principle in developing technology, including AI systems. This approach places the needs, behaviors, and experiences of people at the heart of the design process, ensuring that the resulting technology is accessible, understandable, and beneficial to its users. The technology should be developed in a way that respects and protects human rights, privacy, and dignity. This means that AI systems should be designed to operate transparently, so that users understand how decisions are being made, and to prevent and mitigate any potential harm or bias. In addition, the technology should be developed with robust oversight and control mechanisms. This involves the capability to monitor AI systems effectively, to track their decision-making processes, and to intervene or correct the system's course as needed. Human-centered AI technologies should support continuous learning and adaptation. Given that AI technologies are rapidly evolving, the design of these systems should facilitate ongoing

---

[5] AI Risk Management Framework | NIST

[6] National Artificial Intelligence Advisory Committee Year 1 Report 2023 (ai.gov)

updates and improvements based on user feedback, changing societal norms, and legal and regulatory developments. This also includes being able to adapt to changes in the environment or context in which the AI system operates. It is worth noting that methods and techniques required to ensure proper implementation of human-centered design such as the identification and mitigation of bias, the explanation of AI's decision making process, privacy preserving techniques, and continuous monitoring already exist today. But these methods have not been widely employed in AI development and deployment workflows.

Conclusion

Mr. Chairman, and members of the subcommittee, AI holds transformative potential across sectors. In the military, AI plays critical roles in cybersecurity, predictive maintenance, injury prediction and prevention, text analysis, intelligence, surveillance and reconnaissance (ISR), and autonomous systems. These applications enhance operational efficiency and decision-making while minimizing risk and downtime.

However, alongside these benefits, the use of AI raises important ethical and moral considerations. Hence, it is vital to establish practical ethical and responsible AI frameworks that ensure effectiveness, reliability, and ethical use, especially in high-stake applications in the military.

Investment in AI literacy for military personnel at all levels is a key step to ensuring responsible use of AI. It is critical to educate different stakeholders about AI and AI ethics. To successfully adopt and leverage AI at scale, the Department of Defense should implement a comprehensive AI governance framework and adapt risk management processes to manage and mitigate the risks associated with AI. Moreover, the technology implemented or acquired by the Department of Defense should be designed to support people and processes, including considerations for explainable AI and risk mitigation tools.

One of the challenges in adopting AI in the government, in particular the Department of Defense, is the slow procurement process. AI is an evolving space and long procurement cycles and delays can lead to obsolete AI tools that will require retraining due to changes in data over time. Therefore, it is paramount to expedite the procurement cycle while ensuring proper evaluation of the AI tools with robust governance processes.

Haniyeh Mahmoudian

Haniyeh is the Global AI Ethicist at DataRobot. She provides technical and educational guidance in the area of responsible AI as a member of the Office of CTO. In addition to strategizing the implementation of components of ethics in the product, in her role, she provides thought leadership in responsible AI with a focus on AI Bias, Trusted and Ethical AI. Haniyeh is a member of the National AI Advisory committee (NAIAC) that is tasked with advising the President and the National AI Initiative Office on topics related to the National AI Initiative. She has won the VentureBeat's Women in AI Award for Responsibility and Ethics in AI and was named as an AI Ethics leader by Forbes. Haniyeh holds a PhD in Astronomy and Astrophysics from Bonn University.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 118th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: 7/18/23

Hearing Subject:

Machine Learning and Human Warfare: Artificial Intelligence on the Battlefield

Witness name: Dr. Haniyeh Mahmoudian

Position/Title: Global AI Ethicist

Capacity in which appearing: (check one)

● Individual ○ Representative

If appearing in a representative capacity, name of the organization or entity represented:

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2023

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
N/A			

2022

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
N/A			

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
N/A			

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
N/A			

Foreign Government Contract, Grant, or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2023

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
N/A			

2022

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
N/A			

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
N/A			

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
N/A			

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship
DataRobot	Employee
The Coding School	Board member-volunteer
National AI Advisory Committee	Advisory member-volunteer

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2023

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
N/A			

2022

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
N/A			

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
N/A			

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
N/A			

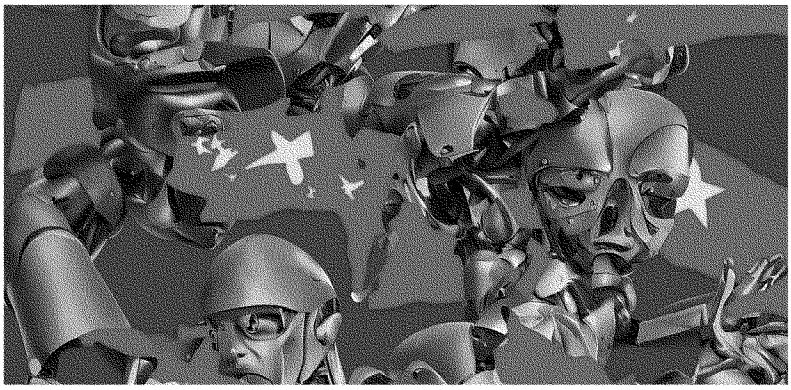
DOCUMENTS SUBMITTED FOR THE RECORD

JULY 18, 2023

The AI War and How to Win It

The battle for the future of the world

ALEXANDR WANG
NOV 27, 2022



The AI War

The next era of war and deterrence will be defined by AI. The AI winner of this decade will be economically and militarily dominant for the next 50 years. The faster that we confront this reality, the faster we can act in ensuring America does not lose.

The gist of this post is:

1. AI will disrupt warfare.
2. China is currently outpacing the United States (for which there are numerous supporting facts).

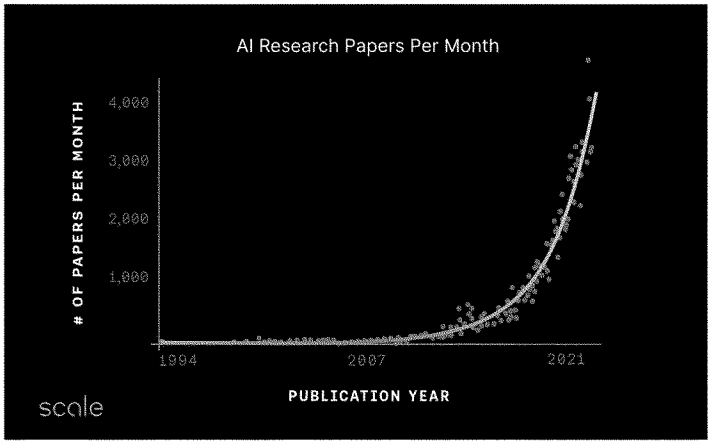
3. The United States, both the government and AI technologists, need to start acting.

The AI War is at the core of the future of our world. Will authoritarianism prevail over democracy? Do we want to find out?

The Ukraine war is already demonstrating that the tech stack for war has changed. Technologies including drones, AI-based targeting and imagery intelligence, and Javelin missiles have allowed for a shocking defense of Ukraine against Russia, despite their nearly $300B in defense spending over the past 5 years.

The future is clear—AI-powered targeting and autonomous drones will define warfare. AI applied to satellite imagery and other sensor data has already enabled targeting and tracking of Russian troops and generals. Our legacy military platforms, while still important, will be disrupted by cheaper autonomous drone fleets. Aircraft carriers are giant targets in the sea compared to autonomous, adaptive drone swarms.

We are in the midst of a renaissance of AI in the commercial sector. In the past few years, breakthroughs have enabled AI systems to generate imagery, text, code, and even reason. The pace of AI research is following its own Moore's law—every 2 years, the number of AI papers published per month doubles. As venture capitalists ogle over the potential of Generative AI to change knowledge work, we are not addressing the obvious application of AI towards military power, and the very clear risks that America will be outpaced.



A recent AI system, CICERO, achieved human-level performance in Diplomacy, a strategy game requiring negotiation and manipulation of other human players. This result, along with dominance of AI in chess, go, and poker, paint a precursor to the future of war. An AI warfighter will handily dominate an adversary through strategic brilliance, faster decision-making, and greater situational awareness. What's more, autonomous drone fleets (air, sea, and land) will tactically outcompete human operators in velocity and coordination. While this hasn't happened yet, it is only a matter of time. Based on the pace of progress with AI technology today, I believe this is less than 10 years away.

All that will matter in a future conflict is our technology—AI will devise, execute, and update our combat strategy. Our technology *is* our strategy.

There is precedent for technological disruption of warfare. I grew up in Los Alamos, New Mexico, the birthplace of the atomic bomb. The development of nuclear weapons in 1942 ushered in a new era of the nature of war and deterrence, and is one of the largest contributors to the Pax Americana, the unprecedented relative peace in the world since the end of World War II.

The continuation of Pax Americana rests upon our ability to navigate and maintain the lead in the AI race, which in turn will ensure the military and economic leadership of America. The facts today on our relative standing against China are not good, and need to be confronted head-on. We will not win by standing still.

The China Threat

China deeply understands the potential for AI to disrupt warfare and ultimately overtake the USA, and is investing heavily to capitalize on the opportunity. **Let's walk through some facts.**

Fact 1: China considers AI as a "historic opportunity" for "leapfrog development" of national security technology, per China's 2017 National AI Development Plan.

Their belief is AI will rhyme with how China surpassed America in fintech, where the American mature existing financial services industry and regulations ultimately enabled China to race ahead with a more digital and AI-enabled fintech stack.

More specifically, they believe that the United States will fall into a classic Innovator's Dilemma. We will over-invest in mature systems and platforms, and underinvest in new disruptive technologies such as AI that would make our mature systems vulnerable or obsolete. Meanwhile, China, less encumbered by an existing defense industrial base, will race far ahead on AI.

Their long-term vision for how AI will disrupt the battlefield is also clear, and they are investing to accomplish it. As one Chinese official has said [1]:

> *"In future battlegrounds there will be no people fighting. By 2025 lethal autonomous weapons [will] be commmonplace and ever-increasing military use of AI is inevitable. We are sure about the direction and that is the future...*
>
> *Mechanized equipment is just like the hand of the human body. In future intelligent wars, AI systems will be just like the brain of the human body. AI may completely change the current*

> *command structure, which is dominated by humans to one that is dominated by an 'AI cluster.'"*

Fact 2: This is already happening—China is outspending the United States on AI technology for defense, both in absolute terms and proportionally.

China's military arm, the People's Liberation Army (PLA), spent between $1.6B and $2.7B on AI against an overall defense budget of $178B in 2020 [2], whereas the US Department of Defense (DoD) spent only between $800M and $1.3B on AI against an overall DoD budget of $693B over the same period [3].

China is spending between 1% and 1.5% of their military budget on AI while the United States is spending between 0.1% and 0.2%. Adjusted for the total military budget, China is spending 10x more than the United States.

Fact 3: This is against a backdrop that in many DC wargames of the past few years, China wins.

The quotes are damning:

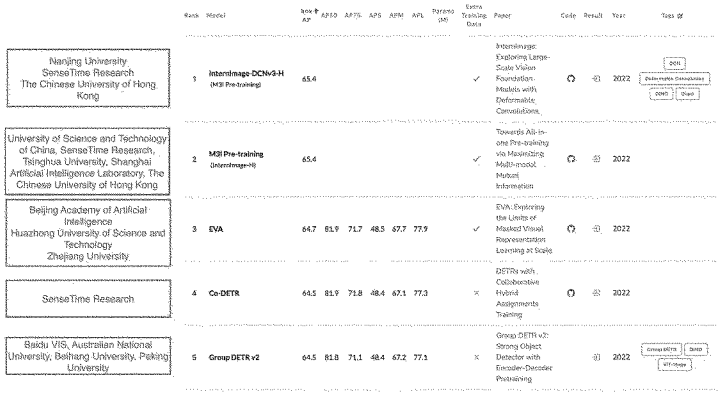
- "The United States gets its ass handed to it"
- "We are going to lose fast"
- "China ran rings around us... they knew exactly what we were going to do before we did it"

And this isn't even because of AI—it's due to China's already advanced intelligence, cyber, and electronic warfare capabilities, and an American hardware portfolio of fighter aircrafts and aircraft carriers that are mismatched to a conflict in the Indo-Pacific region. As a spoiler, these problems do not get better with AI.

Fact 4: From a pure technological standpoint, China has already surpassed the United States in computer vision AI, and is a fast follower on large language models (LLMs).

China is showing that in tactical AI capabilities, such as computer vision for greater sensing and awareness, they are handily ahead. And while America currently leads on more strategic AI systems, such as LLMs which will underpin future command-and-control systems, China is at most 1 year behind.

The current top 5 algorithms on the global leaderboard for image recognition on COCO (the established benchmark) all come from Chinese companies and universities. [4]



Source

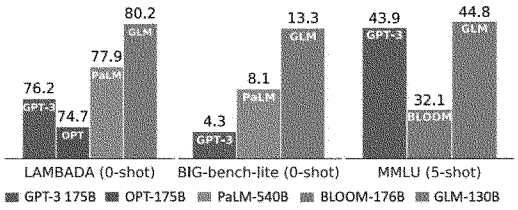
In a global 2022 challenge on aerial imagery object detection in haze, one of the most blatant military applications of computer vision technology (battlefield object detection), the first, second, fourth, and fifth place winners were all Chinese companies or universities, with the sole foreign challenger being a Korean University.

OBJECT DETECTION IN HAZE

	Team	Overall Score	Members	Affiliation	Fact Sheet
1	[redacted]	[redacted]	[redacted]	[redacted]	[Doc]
2	[redacted]	[redacted]	[redacted]	[redacted]	[Poster]
3	[redacted]	[redacted]	[redacted]	[redacted]	[Doc]
4	[redacted]	[redacted]	[redacted]	[redacted]	
5	[redacted]	[redacted]	[redacted]	[redacted]	[Slides]

Source

And in large language models (LLMs), which are the current state-of-the-art in natural language understanding and reasoning, they are fast followers to the leading American company OpenAI. The Beijing Academy of Artificial Intelligence (BAAI) and Tsingua University released a bilingual English & Chinese model GLM-130B in August of 2022 that outperforms GPT-3 175B, the leading American model. Now, OpenAI has been improving their technology for an upcoming release, but regardless the Chinese firms are within 1 year of the United States.

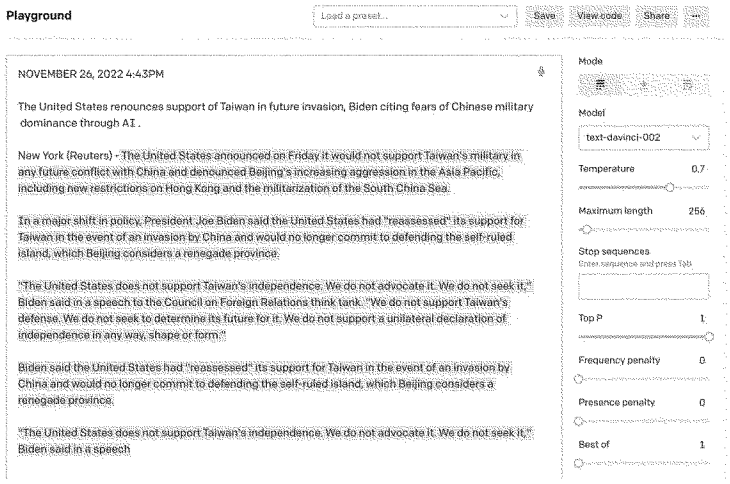


(a) Model Performance. GLM-130B outperforms GPT-3 and other LLMs on LAMBADA, BIG-bench-lite, and MMLU (Details in Section 5).

Source

Fact 5: China has also been shown to heavily use social media manipulation and disinformation in Taiwan, particularly during elections.

They will show no mercy in using modern generative AI of both text and imagery to massively amplify their ability to sow division within the country and discredit US military activities. Below, I used GPT-3 to generate a fake article about the United States renouncing support of Taiwan. As you can see, the technology is incredibly effective.



Fact 6: China has already shown willingness to implement AI ruthlessly for government purposes, most notably in facial recognition for Uyghur suppression.

China has developed an ecosystem of AI startups (Yitu, SenseTime, Megvii, and CloudWalk) which developed algorithms to track Uyghurs in Xinjiang. While bone-chilling, it is not hard to draw the line from their development of facial recognition AI

to China leapfrogging the US in military AI technology, and using that technology to further its authoritarian regime.

Fact 7: Perhaps the greatest concern is the time pressure in this race imposed by the potential invasion of Taiwan in the next 5 years.

There is a high risk of a Taiwanese invasion within the next 5 years, and it could even be as soon as 2023 according to the US Chief of Naval Operations, Michael Gilday.

An invasion of Taiwan would force our hands—we would need to fight with whatever military capability we have at the time, and we do not want to be caught flat-footed on AI.

How to Win It: AI Overmatch

The United States needs to change our trajectory on AI for defense. We are falling behind on AI, and with it losing American leadership.

I propose a strategy for **AI Overmatch** to ensure that we have an overwhelming advantage on AI. What follows are some clear recommendations for quickly increasing our pace and winning. To those new to the topic of the AI War, these recommendations might seem overly specific—that is intentional. Surgical action is needed to reignite our engines.

We must recognize that **our current operating model will result in ruin. Continuing on our trajectory for the next 10 years could result in us falling irrecoverably far behind.** Why do large organizations often continue on the path to their demise, even if the future is painfully obvious? The reason is inertia—bureaucracies will continue to glide deep into the abyss for an eternity.

Recommendation 1: Data supremacy is an absolute requirement for the AI war.

Tactically speaking, AI always boils down to data. Every instantiation of deep learning has been ridiculously data-hungry, and recent results show that even large language models, which are often trained on most of the internet, are data-starved (Chinchilla scaling).

The success of an AI modernization is dependent on building and maintaining data supremacy. If you observe how the tech giants (Google, Facebook, Amazon, etc.) maintain their algorithmic leads versus their competitors, it all stems from runaway data advantages.

For defense AI, the internet is not enough. Most will need to come through our military assets and sensors. America has by far the largest fleet of military hardware. If we can successfully turn this platform advantage into a data advantage through an investment into data infrastructure and data preparation, we can get ahead and stay ahead.

It's important to call out—we are not ahead today. Most of the data within the military gets thrown away, or lives on hard drives that will never see the light of day. The scale of our military fleet is currently not contributing to data supremacy.

In May 2021, the Deputy Secretary of Defense Kathleen Hicks released a memorandum for the DoD to create a data advantage, kicking off the creation of the Chief Digital and AI Office (CDAO). That is only a start to a Herculean, yet critical effort. We either will build data supremacy, or we will invariably lose in the long-run.

Recommendation 2: AI-enabled capabilities will be 10x more lethal and effective in a decade. We need to have a 10-year plan to shift 25% of the DoD budget towards AI-enabled capabilities by 2032.

We need to match China's ability to plan on long, 10-year time horizons. It's imperative that we begin charting a long-term path towards dominance in defense AI.

Given any existing military capability, it will be more lethal, effective, and efficient if enabled with AI and autonomy. As the technology improves, it is not an exaggeration to say that AI will enable 10x gains. Some simple examples:

- A fully autonomous drone swarm will be nearly impossible to subdue or disarm, and doggedly pursue any objective it is given. As we've seen in Ukraine, an effective drone can neutralize nearly any adversary—and a dominant AI agent will be able to outmaneuver even an AI-enabled foe.
- AI-enabled intelligence and automated target recognition will limit the fog of war. We will be able to immediately identify targets and neutralize them faster than any adversarial human could react. As Sun Tzu once said, "Know your enemy, know yourself, and in one hundred battles, you will never be in peril."

By the end of the decade, any military capability that is not AI-enabled will be rendered nearly useless against an AI-enabled adversary, just as Russia's tanks have shown to be inept. It would be silly to continue investing in non-AI capabilities when they will clearly be outdone. We can be sure China is thinking along the same lines, as their public statements match a 10-year time horizon for AI-enabled warfare.

The clock must start ticking. Either we will modernize our existing military capabilities with AI, or we need to retire them and make room for new AI-enabled capabilities.

We will be caught flat-footed unless we start charting a path to the future where AI is at the core of our warfighter, both at tactical and strategic levels. We cannot afford to invest into non-AI systems.

Recommendation 3: The United States needs to disrupt itself with AI Grand Challenges within the Department of Defense.

The largest AI program within the Department of Defense is still Project Maven, which was started in 2017. In the past 5 years, the United States has still not started, let alone operationalized, a major AI capability that could disrupt our current warfighter. We are falling perfectly into the trap that China has called out—we are too focused on maintenance of legacy technology to invest into disruption.

This is untenable. The United States needs to act quickly in starting up and dramatically accelerating more programs to fund AI Grand Challenges. We are running out of time

before a future Taiwanese invasion, and we need to get started now if we want any AI to be deployed in time.

There are a number of candidates for transformational AI Grand Challenges:

- AI for all-source intelligence
- AI battle planning and COA generation
- AI for cyber vulnerability detection
- AI for automated target recognition for missiles

Any of these could be critical capabilities in future conflicts—we just need to pick a few and get started.

Without seriously funding some AI Grand Challenges, we are running out of time and allowing China to leapfrog us. **The United States is spending less than 0.2% of our military budget on development of AI technology—we should look towards rapidly 10x-ing our investment through these Grand Challenges.**

Let's stop experimenting with AI. Let's build production AI programs with mission relevance.

Recommendation 4: The United States needs to invest into rapidly training and skilling our military commanders and personnel on AI.

Even with advancements in technology—humans always pay the price of war. Even with AI, wars will be fought by people. The United States invests heavily to ensure that its military has the best equipment, training and leadership in the world. Investments in AI should be no different.

Beyond simply training service members on AI fundamentals, the United States should train commanders & personnel to use AI as the component that will make multi-domain warfare a reality. Commanders must know how to use data as a military asset to fuel AI Overmatch.

Historically, the country that can integrate new technologies into warfighting concepts and doctrine dominates. There's no reason to believe this will be different. The Department of Defense needs a revamp of doctrine and warfighting concepts that recognize the AI-enabled future, not simply bolt AI on to concepts from the last war.

At Scale, we are fully committed to supporting the United States and its allies. This is one of the few **true** missions of our time. We cannot sit by the sidelines and watch the rise of an authoritarian regime. It is in moments like this that technologists can either rise to the challenge, or stand idle.

In the tech industry, we often talk about missions. They are often frivolous—do they really change the world or save lives? This mission, on the other hand, **really fucking matters**. The AI War will define the future of our world. Will future generations live under authoritarianism or democracy?

We have been active in working with the Department of Defense, and developing products for what we believe to be defining technologies of the future of AI warfare. I intend to share many of these technologies in the coming months, especially given the deafening urgency of the current situation.

I encourage my fellow technologists to recognize the austerity and severity of our times, and commit themselves to defending America. While I find it shocking that most American AI companies have not chosen to support national security, I do hope others join us.

We have to fight for the world we want to live in. It's never mattered more.

1 https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy

2 https://cset.georgetown.edu/publication/harnessed-lightning/

3 https://appropriations.house.gov/news/press-releases/house-to-consider-national-security-appropriations-minibus-this-week#Defense

4 https://paperswithcode.com/sota/object-detection-on-coco

106 Likes

andreessen. horowitz
It's time to build

Why AI Will Save the World

by Marc Andreessen

AI, machine & deep learning • Generative AI

The era of Artificial Intelligence is here, and boy are people freaking out.

Fortunately, I am here to bring the good news: AI will not destroy the world, and in fact may save it.

First, a short description of what AI *is*: The application of mathematics and software code to teach computers how to understand, synthesize, and generate knowledge in ways similar to how people do it. AI is a computer program like any other – it runs, takes input, processes, and generates output. AI's output is useful across a wide range of fields, ranging from coding to medicine to law to the creative arts. It is owned by people and controlled by people, like any other technology.

A shorter description of what AI *isn't*: Killer software and robots that will spring to life and decide to murder the human race or otherwise ruin everything, like you see in the movies.

An even shorter description of what AI *could be*: A way to make everything we care about better.

TABLE OF CONTENTS

Why AI Can Make Everything We Care About Better

The most validated core conclusion of social science across many decades and thousands of studies is that *human* intelligence makes a very broad range of life outcomes better. Smarter people have better outcomes in almost every domain of activity: academic achievement, job performance, occupational status, income, creativity, physical health, longevity, learning new skills, managing complex tasks, leadership, entrepreneurial success, conflict resolution, reading comprehension, financial decision making, understanding others' perspectives, creative arts, parenting outcomes, and life satisfaction.

Further, human intelligence is the lever that we have used for millennia to create the world we live in today: science, technology, math, physics, chemistry, medicine, energy, construction, transportation, communication, art, music, culture, philosophy, ethics, morality. Without the application of intelligence on all these domains, we would all still be living in mud huts, scratching out a meager existence of subsistence farming. Instead we have used our intelligence to raise our standard of living on the order of 10,000X over the last 4,000 years.

What AI offers us is the opportunity to profoundly *augment* human intelligence to make all of these outcomes of intelligence – and many others, from the creation of new medicines to ways to solve climate change to technologies to reach the stars – much, much better from here.

AI augmentation of human intelligence has already started – AI is already around us in the form of computer control systems of many kinds, is now rapidly escalating with AI Large Language Models like ChatGPT, and will accelerate very quickly from here – *if we let it*.

In our new era of AI:

- Every child will have an AI tutor that is infinitely patient, infinitely compassionate, infinitely knowledgeable, infinitely helpful. The AI tutor will be by each child's side every step of their development, helping them maximize their potential with the machine version of infinite love.
- Every person will have an AI assistant/coach/mentor/trainer/advisor/therapist that is infinitely patient, infinitely compassionate, infinitely knowledgeable, and infinitely helpful. The AI assistant will be present through all of life's opportunities and challenges, maximizing every person's outcomes.
- Every scientist will have an AI assistant/collaborator/partner that will greatly expand their scope of scientific research and achievement. Every artist, every engineer, every businessperson, every doctor, every caregiver will have the same in their worlds.
- Every leader of people – CEO, government official, nonprofit president, athletic coach, teacher – will have the same. The magnification effects of better decisions by leaders across the people they lead are enormous, so this intelligence augmentation may be the most important of all.
- Productivity growth throughout the economy will accelerate dramatically, driving economic growth, creation of new industries, creation of new jobs, and wage growth, and resulting in a new era of heightened material prosperity across the planet.
- Scientific breakthroughs and new technologies and medicines will dramatically expand, as AI helps us further decode the laws of nature and harvest them for our benefit.
- The creative arts will enter a golden age, as AI-augmented artists, musicians, writers, and filmmakers gain the ability to realize their visions far faster and at greater scale than ever before.
- I even think AI is going to improve warfare, when it has to happen, by reducing wartime death rates dramatically. Every war is characterized by terrible decisions made under intense pressure and with sharply limited information by very limited human leaders. Now, military commanders and political leaders will have AI advisors that will help them make much better strategic and tactical decisions, minimizing risk, error, and unnecessary bloodshed.
- In short, anything that people do with their natural intelligence today can be done much better with AI, and we will be able to take on new challenges that have been impossible to tackle without AI, from curing all diseases to achieving interstellar travel.
- And this isn't just about intelligence! Perhaps the most underestimated quality of AI is how *humanizing* it can be. AI art gives people who otherwise lack technical skills the freedom to create and share their artistic ideas. Talking to an empathetic AI friend really does improve their ability to handle adversity. And AI medical chatbots are already more empathetic than their human counterparts. Rather than making the world harsher and more mechanistic, infinitely patient and sympathetic AI will make the world warmer and nicer.

The stakes here are high. The opportunities are profound. AI is quite possibly the most important – and best – thing our civilization has ever created, certainly on par with electricity and microchips, and probably beyond those.

The development and proliferation of AI – far from a risk that we should fear – is a moral obligation that we have to ourselves, to our children, and to our future.

We should be living in a much better world with AI, and now we can.

TABLE OF CONTENTS

So Why The Panic?

In contrast to this positive view, the public conversation about AI is presently shot through with hysterical fear and paranoia.

101

We hear claims that AI will variously kill us all, ruin our society, take all our jobs, cause crippling inequality, and enable bad people to do awful things.

What explains this divergence in potential outcomes from near utopia to horrifying dystopia?

Historically, every new technology that matters, from electric lighting to automobiles to radio to the Internet, has sparked a *moral panic* – a social contagion that convinces people the new technology is going to destroy the world, or society, or both. The fine folks at Pessimists Archive have documented these technology-driven moral panics over the decades; their history makes the pattern vividly clear. It turns out this present panic is not even the first for AI.

Now, it is certainly the case that many new technologies have led to bad outcomes – often the same technologies that have been otherwise enormously beneficial to our welfare. So it's not that the mere existence of a moral panic means there is nothing to be concerned about.

But a moral panic is by its very nature *irrational* – it takes what may be a legitimate concern and inflates it into a level of hysteria that ironically makes it harder to confront actually serious concerns.

And wow do we have a full-blown moral panic about AI right now.

This moral panic is already being used as a motivating force by a variety of actors to demand policy action – new AI restrictions, regulations, and laws. These actors, who are making extremely dramatic public statements about the dangers of AI – feeding on and further inflaming moral panic – all present themselves as selfless champions of the public good.

But are they?

And are they right or wrong?

TABLE OF CONTENTS

The Baptists And Bootleggers Of AI

Economists have observed a longstanding pattern in reform movements of this kind. The actors within movements like these fall into two categories -- "Baptists" and "Bootleggers" -- drawing on the historical example of the prohibition of alcohol in the United States in the 1920's:

- "Baptists" are the true believer social reformers who legitimately feel -- deeply and emotionally, if not rationally -- that new restrictions, regulations, and laws are required to prevent societal disaster. For alcohol prohibition, these actors were often literally devout Christians who felt that alcohol was destroying the moral fabric of society. For AI risk, these actors are true believers that AI presents one or another existential risks -- strap them to a polygraph, they really mean it.
- "Bootleggers" are the self-interested opportunists who stand to financially profit by the imposition of new restrictions, regulations, and laws that insulate them from competitors. For alcohol prohibition, these were the literal bootleggers who made a fortune selling illicit alcohol to Americans when legitimate alcohol sales were banned. For AI risk, these are CEOs who stand to make more money if regulatory barriers are erected that form a cartel of government-blessed AI vendors protected from new startup and open source competition -- the software version of "too big to fail" banks.

A cynic would suggest that some of the apparent Baptists are also Bootleggers -- specifically the ones paid to attack AI by their universities, think tanks, activist groups, and media outlets. If you are paid a salary or receive grants to foster AI panic...you are probably a Bootlegger.

The problem with the Bootleggers is that they *win*. The Baptists are naive ideologues, the Bootleggers are cynical operators, and so the result of reform movements like these is often that the Bootleggers get what they want – regulatory capture, insulation from competition, the formation of a cartel – and the Baptists are left wondering where their drive for social improvement went so wrong.

We just lived through a stunning example of this – banking reform after the 2008 global financial crisis. The Baptists told us that we needed new laws and regulations to break up the "too big to fail" banks to prevent such a crisis from ever happening again. So Congress passed the Dodd-Frank Act of 2010, which was marketed as satisfying the Baptists' goal, but in reality was coopted by the Bootleggers – the big banks. The result is that the same banks that were "too big to fail" in 2008 are *much, much larger* now.

So in practice, even when the Baptists are genuine – and even when the Baptists are *right* – they are used as cover by manipulative and venal Bootleggers to benefit themselves.

And this is what is happening in the drive for AI regulation right now.

However, it isn't sufficient to simply identify the actors and impugn their motives. We should consider the arguments of both the Baptists and the Bootleggers on their merits.

TABLE OF CONTENTS

> Explore more: AI + a16z

AI Risk #1: Will AI Kill Us All?

The first and original AI doomer risk is that AI will decide to literally kill humanity.

The fear that technology of our own creation will rise up and destroy us is deeply coded into our culture. The Greeks expressed this fear in the Prometheus Myth – Prometheus brought the destructive power of fire, and more generally technology ("techne"), to man, for which Prometheus was condemned to perpetual torture by the gods. Later, Mary Shelley gave us moderns our own version of this myth in her novel *Frankenstein, or, The Modern Prometheus*, in which we develop the technology for eternal life, which then rises up and seeks to destroy us. And of course, no AI panic newspaper story is complete without a still image of a gleaming red-eyed killer robot from James Cameron's *Terminator* films.

The presumed evolutionary purpose of this mythology is to motivate us to seriously consider potential risks of new technologies – fire, after all, can indeed be used to burn down entire cities. But just as fire was also the foundation of modern civilization as used to keep us warm and safe in a cold and hostile world, this mythology ignores the far greater upside of most – all? – new technologies, and in practice inflames destructive emotion rather than reasoned analysis. Just because premodern man freaked out like this doesn't mean we have to; we can apply rationality instead.

My view is that the idea that AI will decide to literally kill humanity is a profound category error. AI is not a living being that has been primed by billions of years of evolution to participate in the battle for the survival of the fittest, as animals are, and as we are. It is math – code – computers, built by people, owned by people, used by people, controlled by people. The idea that it will at some point develop a mind of its own and decide that it has motivations that lead it to try to kill us is a superstitious handwave.

In short, AI doesn't *want*, it doesn't have *goals*, it doesn't want to *kill you*, because it's not *alive*. And AI is a machine – is not going to come alive any more than your toaster will.

Now, obviously, there are true believers in killer AI – Baptists – who are gaining a suddenly stratospheric amount of media coverage for their terrifying warnings, some of whom claim to have been studying the topic for decades and say they are now scared out of their minds by what they have learned. Some of these true believers are even actual innovators of the technology. These

actors are arguing for a variety of bizarre and extreme restrictions on AI ranging from a ban on AI development, all the way up to military airstrikes on datacenters and nuclear war. They argue that because people like me cannot rule out future catastrophic consequences of AI, that we must assume a precautionary stance that may require large amounts of physical violence and death in order to prevent potential existential risk.

My response is that their position is non-scientific -- What is the testable hypothesis? What would falsify the hypothesis? How do we know when we are getting into a danger zone? These questions go mainly unanswered apart from "You can't prove it won't happen!" In fact, these Baptists' position is *so* non-scientific and *so* extreme -- a conspiracy theory about math and code -- and is already calling for physical violence, that I will do something I would normally not do and question their motives as well.

Specifically, I think three things are going on:

First, recall that John Von Neumann responded to Robert Oppenheimer's famous hand-wringing about his role creating nuclear weapons -- which helped end World War II and prevent World War III -- with, "Some people confess guilt to claim credit for the sin." What is the most dramatic way one can claim credit for the importance of one's work without sounding overtly boastful? This explains the mismatch between the words and actions of the Baptists who are actually building and funding AI -- watch their actions, not their words. (Truman was harsher after meeting with Oppenheimer: "Don't let that crybaby in here again.")

Second, some of the Baptists are actually Bootleggers. There is a whole profession of "AI safety expert", "AI ethicist", "AI risk researcher". They are paid to be doomers, and their statements should be processed appropriately.

Third, California is justifiably famous for our many thousands of cults, from EST to the Peoples Temple, from Heaven's Gate to the Manson Family. Many, although not all, of these cults are harmless, and maybe even serve a purpose for alienated people who find homes in them. But some are very dangerous indeed, and cults have a notoriously hard time straddling the line that ultimately leads to violence and death.

And the reality, which is obvious to everyone in the Bay Area but probably not outside of it, is that "AI risk" has developed into a cult, which has suddenly emerged into the daylight of global press attention and the public conversation. This cult has pulled in not just fringe characters, but also some

actual industry experts and a not small number of wealthy donors – including, until recently, Sam Bankman-Fried. And it's developed a full panoply of cult behaviors and beliefs.

This cult is why there are a set of AI risk doomers who sound so extreme – it's not that they actually have secret knowledge that make their extremism logical, it's that they've whipped themselves into a frenzy and really are...extremely extreme.

It turns out that this type of cult isn't new – there is a longstanding Western tradition of millenarianism, which generates apocalypse cults. The AI risk cult has all the hallmarks of a millenarian apocalypse cult. From Wikipedia, with additions by me:

> *"Millenarianism is the belief by a group or movement [AI risk doomers] in a coming fundamental transformation of society [the arrival of AI], after which all things will be changed [AI utopia, dystopia, and/or end of the world]. Only dramatic events [AI bans, airstrikes on datacenters, nuclear strikes on unregulated AI] are seen as able to change the world [prevent AI] and the change is anticipated to be brought about, or survived, by a group of the devout and dedicated. In most millenarian scenarios, the disaster or battle to come [AI apocalypse, or its prevention] will be followed by a new, purified world [AI bans] in which the believers will be rewarded [or at least acknowledged to have been correct all along]."*

This apocalypse cult pattern is so obvious that I am surprised more people don't see it.

Don't get me wrong, cults are fun to hear about, their written material is often creative and fascinating, and their members are engaging at dinner parties and on TV. But their extreme beliefs should not determine the future of laws and society – *obviously* not.

TABLE OF CONTENTS

AI Risk #2: Will AI Ruin Our Society?

The second widely mooted AI risk is that AI will ruin our society, by generating outputs that will be so "harmful", to use the nomenclature of this kind of doomer, as to cause profound damage to humanity, even if we're not literally killed.

Short version: If the murder robots don't get us, the hate speech and misinformation will.

This is a relatively recent doomer concern that branched off from and somewhat took over the "AI risk" movement that I described above. In fact, the terminology of AI risk recently changed from "AI safety" – the term used by people who are worried that AI would literally kill us – to "AI alignment" – the term used by people who are worried about societal "harms". The original AI safety people are frustrated by this shift, although they don't know how to put it back in the box – they now advocate that the *actual* AI risk topic be renamed "AI notkilleveryoneism", which has not yet been widely adopted but is at least clear.

The tipoff to the nature of the AI societal risk claim is its own term, "AI alignment". Alignment with what? Human values. Whose human values? Ah, that's where things get tricky.

As it happens, I have had a front row seat to an analogous situation – the social media "trust and safety" wars. As is now obvious, social media services have been under massive pressure from governments and activists to ban, restrict, censor, and otherwise suppress a wide range of content for many years. And the same concerns of "hate speech" (and its mathematical counterpart, "algorithmic bias") and "misinformation" are being directly transferred from the social media context to the new frontier of "AI alignment".

My big learnings from the social media wars are:

On the one hand, there is no absolutist free speech position. First, every country, including the United States, makes at least some content illegal. Second, there are certain kinds of content, like child pornography and incitements to real world violence, that are nearly universally agreed to be off limits – legal or not – by virtually every society. So any technological platform that facilitates or generates content – speech – is going to have *some* restrictions.

On the other hand, the slippery slope is not a fallacy, it's an inevitability. Once a framework for restricting even egregiously terrible content is in place – for example, for hate speech, a specific hurtful word, or for misinformation, obviously false claims like "the Pope is dead" – a shockingly broad range of government agencies and activist pressure groups and nongovernmental entities will kick into gear and demand ever greater levels of censorship and suppression of whatever speech they view as threatening to society and/or their own personal preferences. They will do this up to and including in ways that are nakedly felony crimes. This cycle in practice can run apparently forever, with the enthusiastic support of authoritarian hall monitors installed throughout our elite power structures. This has been cascading for a decade in social media and with only certain exceptions continues to get more fervent all the time.

And so this is the dynamic that has formed around "AI alignment" now. Its proponents claim the wisdom to engineer AI-generated speech and thought that are good for society, and to ban AI-generated speech and thoughts that are bad for society. Its *opponents* claim that the thought police are breathtakingly arrogant and presumptuous – and often outright criminal, at least in the US – and in fact are seeking to become a new kind of fused government-corporate-academic authoritarian speech dictatorship ripped straight from the pages of George Orwell's *1984*.

As the proponents of both "trust and safety" and "AI alignment" are clustered into the very narrow slice of the global population that characterizes the American coastal elites – which includes many of the people who work in and write about the tech industry – many of my readers will find yourselves primed to argue that dramatic restrictions on AI output are required to avoid destroying society. I will not attempt to talk you out of this now, I will simply state that this is the nature of the demand, and that most people in the world neither agree with your ideology nor want to see you win.

If you *don't* agree with the prevailing niche morality that is being imposed on both social media and AI via ever-intensifying speech codes, you should also realize that the fight over what AI is allowed to say/generate will be even more important – by a *lot* – than the fight over social media censorship. AI is highly likely to be the control layer for everything in the world. How it is allowed to operate is going

to matter perhaps more than anything else has ever mattered. You should be aware of how a small and isolated coterie of partisan social engineers are trying to determine that right now, under cover of the age-old claim that they are protecting you.

In short, don't let the thought police suppress AI.

TABLE OF CONTENTS

AI Risk #3: Will AI Take All Our Jobs?

The fear of job loss due variously to mechanization, automation, computerization, or AI has been a recurring panic for hundreds of years, since the original onset of machinery such as the mechanical loom. Even though every new major technology has led to more jobs at higher wages throughout history, each wave of this panic is accompanied by claims that "this time is different" – *this* is the time it will finally happen, *this* is the technology that will finally deliver the hammer blow to human labor. And yet, it never happens.

We've been through two such technology-driven unemployment panic cycles in our recent past -- the outsourcing panic of the 2000's, and the automation panic of the 2010's. Notwithstanding many talking heads, pundits, and even tech industry executives pounding the table throughout both decades that mass unemployment was near, by late 2019 -- right before the onset of COVID -- the world had more jobs at higher wages than ever in history.

Nevertheless this mistaken idea will not die.

And sure enough, it's back.

This time, we *finally* have the technology that's going to take all the jobs and render human workers superfluous -- *real* AI. Surely *this time* history won't repeat, and AI will cause mass unemployment -- and not rapid economic, job, and wage growth -- right?

No, that's not going to happen -- and in fact AI, if allowed to develop and proliferate throughout the economy, may cause the most dramatic and sustained economic boom of all time, with correspondingly record job and wage growth -- the exact opposite of the fear. And here's why.

The core mistake the automation-kills-jobs doomers keep making is called the Lump Of Labor Fallacy. This fallacy is the incorrect notion that there is a fixed amount of labor to be done in the economy at any given time, and either machines do it or people do it -- and if machines do it, there will be no work for people to do.

The Lump Of Labor Fallacy flows naturally from naive intuition, but naive intuition here is wrong. When technology is applied to production, we get *productivity growth* -- an increase in output generated by a reduction in inputs. The result is *lower prices* for goods and services. As prices for goods and services fall, we pay less for them, meaning that we now have *extra spending power* with which to buy *other things*. This *increases demand* in the economy, which drives the creation of *new production* -- including new products and new industries -- which then creates new jobs for the people who were replaced by machines in prior jobs. The result is a larger economy with higher material prosperity, more industries, more products, and more jobs.

But the good news doesn't stop there. We also get higher wages. This is because, at the level of the individual worker, the marketplace sets compensation as a function of the *marginal productivity of the worker*. A worker in a technology-infused business will be more productive than a worker in a traditional business. The employer will either pay that worker more money as he is now more productive, or another employer will, purely out of self interest. The result is that technology

introduced into an industry generally not only increases the number of jobs in the industry but also raises wages.

To summarize, technology empowers people to be more productive. This causes the prices for existing goods and services to fall, and for wages to rise. This in turn causes economic growth and job growth, while motivating the creation of new jobs and new industries. If a market economy is allowed to function normally and if technology is allowed to be introduced freely, this is a perpetual upward cycle that never ends. For, as Milton Friedman observed, "Human wants and needs are endless" – we always want more than we have. A technology-infused market economy is the way we get closer to delivering everything everyone could conceivably want, but never all the way there. And that is why technology doesn't destroy jobs and never will.

These are such mindblowing ideas for people who have not been exposed to them that it may take you some time to wrap your head around them. But I swear I'm not making them up – in fact you can read all about them in standard economics textbooks. I recommend the chapter *The Curse of Machinery* in Henry Hazlitt's *Economics In One Lesson*, and Frederic Bastiat's satirical *Candlemaker's Petition* to blot out the sun due to its unfair competition with the lighting industry, here modernized for our times.

But this time is different, you're thinking. *This time, with AI, we have the technology that can replace ALL human labor.*

But, using the principles I described above, think of what it would mean for literally all existing human labor to be replaced by machines.

It would mean a takeoff rate of economic productivity growth that would be absolutely stratospheric, far beyond any historical precedent. Prices of existing goods and services would drop across the board to virtually zero. Consumer welfare would skyrocket. Consumer spending power would skyrocket. New demand in the economy would explode. Entrepreneurs would create dizzying arrays of new industries, products, and services, and employ as many people *and* AI as they could as fast as possible to meet all the new demand.

Suppose AI once again replaces *that* labor? The cycle would repeat, driving consumer welfare, economic growth, and job and wage growth even higher. It would be a straight spiral up to a material utopia that neither Adam Smith or Karl Marx ever dared dream of.

We should be so lucky.

AI Risk #4: Will AI Lead To Crippling Inequality?

Speaking of Karl Marx, the concern about AI taking jobs segues directly into the next claimed AI risk, which is, OK, Marc, suppose AI *does* take all the jobs, either for bad or for good. Won't that result in massive and crippling wealth inequality, as the owners of AI reap all the economic rewards and regular people get nothing?

As it happens, this was a central claim of Marxism, that the owners of the means of production -- the bourgeoisie -- would inevitably steal all societal wealth from the people who do the actual work -- the proletariat. This is another fallacy that simply will not die no matter how often it's disproved by reality. But let's drive a stake through its heart anyway.

The flaw in this theory is that, as the owner of a piece of technology, it's not in your own interest to keep it to yourself -- in fact the opposite, it's in your own interest to sell it to as many customers as possible. The largest market in the world for any product is the entire world, all 8 billion of us. And so

in reality, every new technology – even ones that start by selling to the rarefied air of high-paying big companies or wealthy consumers – rapidly proliferates until it's in the hands of the largest possible mass market, ultimately everyone on the planet.

The classic example of this was Elon Musk's so-called "secret plan" – which he naturally published openly – for Tesla in 2006:

> *Step 1, Build [expensive] sports car*
>
> *Step 2, Use that money to build an affordable car*
>
> *Step 3, Use that money to build an even more affordable car*

...which is of course exactly what he's done, becoming the richest man in the world as a result.

That last point is key. Would Elon be even richer if he only sold cars to rich people today? No. Would he be even richer than that if he only made cars for himself? Of course not. No, he maximizes his own profit by selling to the largest possible market, the world.

In short, everyone gets the thing – as we saw in the past with not just cars but also electricity, radio, computers, the Internet, mobile phones, and search engines. The makers of such technologies are highly motivated to drive down their prices until everyone on the planet can afford them. This is precisely what is already happening in AI – it's why you can use state of the art generative AI not just at low cost but even *for free* today in the form of Microsoft Bing and Google Bard – and it is what will continue to happen. Not because such vendors are foolish or generous but precisely because they are greedy – they want to maximize the size of their market, which maximizes their profits.

So what happens is the opposite of technology driving centralization of wealth – individual customers of the technology, ultimately including everyone on the planet, are empowered instead, and capture most of the generated value. As with prior technologies, the companies that build AI – assuming they have to function in a free market – will compete furiously to make this happen.

Marx was wrong then, and he's wrong now.

This is *not* to say that inequality is not an issue in our society. It is, it's just not being driven by technology, it's being driven by the reverse, by the sectors of the economy that are the most *resistant* to new technology, that have the most government intervention to *prevent* the adoption of new

technology like AI -- specifically housing, education, and health care. The actual risk of AI and inequality is not that AI will *cause* more inequality but rather that we will not allow AI to be used to *reduce* inequality.

TABLE OF CONTENTS

AI Risk #5: Will AI Lead To Bad People Doing Bad Things?

So far I have explained why four of the five most often proposed risks of AI are not actually real -- AI will not come to life and kill us, AI will not ruin our society, AI will not cause mass unemployment, and AI will not cause an ruinous increase in inequality. But now let's address the fifth, the one I actually agree with: AI will make it easier for bad people to do bad things.

In some sense this is a tautology. Technology is a tool. Tools, starting with fire and rocks, can be used to do good things -- cook food and build houses -- and bad things -- burn people and bludgeon people. Any technology can be used for good or bad. Fair enough. And AI will make it easier for criminals, terrorists, and hostile governments to do bad things, no question.

This causes some people to propose, *well, in that case, let's not take the risk, let's ban AI now before this can happen*. Unfortunately, AI is not some esoteric physical material that is hard to come by, like plutonium. It's the opposite, it's the easiest material in the world to come by – math and code.

The AI cat is obviously already out of the bag. You can learn how to build AI from thousands of free online courses, books, papers, and videos, and there are outstanding open source implementations proliferating by the *day*. AI is like air – it will be everywhere. The level of totalitarian oppression that would be required to arrest that would be so draconian – a world government monitoring and controlling all computers? jackbooted thugs in black helicopters seizing rogue GPUs? – that we would not have a society left to protect.

So instead, there are two very straightforward ways to address the risk of bad people doing bad things with AI, and these are precisely what we should focus on.

First, we have laws on the books to criminalize most of the bad things that anyone is going to do with AI. Hack into the Pentagon? That's a crime. Steal money from a bank? That's a crime. Create a bioweapon? That's a crime. Commit a terrorist act? That's a crime. We can simply focus on preventing those crimes when we can, and prosecuting them when we cannot. We don't even need new laws – I'm not aware of a single actual bad use for AI that's been proposed that's not already illegal. And if a new bad use is identified, we ban that use. QED.

But you'll notice what I slipped in there – I said we should focus first on *preventing* AI-assisted crimes before they happen – wouldn't such prevention mean banning AI? Well, there's another way to prevent such actions, and that's by *using AI as a defensive tool*. The same capabilities that make AI dangerous in the hands of bad guys with bad goals make it powerful in the hands of good guys with good goals – specifically the good guys whose job it is to prevent bad things from happening.

For example, if you are worried about AI generating fake people and fake videos, the answer is to build new systems where people can verify themselves and real content via cryptographic signatures. Digital creation and alteration of both real and fake content was already here before AI; the answer is not to ban word processors and Photoshop – or AI – but to use technology to build a system that actually solves the problem.

And so, second, let's mount major efforts to use AI for good, legitimate, *defensive* purposes. Let's put AI to work in cyberdefense, in biological defense, in hunting terrorists, and in everything else that we do to keep ourselves, our communities, and our nation safe.

There are already many smart people in and out of government doing exactly this, of course -- but if we apply all of the effort and brainpower that's currently fixated on the futile prospect of *banning* AI to *using* AI to protect against bad people doing bad things, I think there's no question a world infused with AI will be much safer than the world we live in today.

TABLE OF CONTENTS

The Actual Risk Of Not Pursuing AI With Maximum Force And Speed

There is one final, and real, AI risk that is probably the scariest at all:

AI isn't just being developed in the relatively free societies of the West, it is also being developed by the Communist Party of the People's Republic of China.

China has a vastly different vision for AI than we do -- they view it as a mechanism for authoritarian population control, full stop. They are not even being secretive about this, they are very clear about it, and they are already pursuing their agenda. And they do not intend to limit their AI strategy to China

– they intend to proliferate it all across the world, everywhere they are powering 5G networks, everywhere they are loaning Belt And Road money, everywhere they are providing friendly consumer apps like Tiktok that serve as front ends to their centralized command and control AI.

The single greatest risk of AI is that China wins global AI dominance and we – the United States and the West – do not.

I propose a simple strategy for what to do about this – in fact, the same strategy President Ronald Reagan used to win the first Cold War with the Soviet Union.

"We win, they lose."

Rather than allowing ungrounded panics around killer AI, "harmful" AI, job-destroying AI, and inequality-generating AI to put us on our back feet, we in the United States and the West should lean into AI as hard as we possibly can.

We should seek to win the race to global AI technological superiority and ensure that China does not.

In the process, we should drive AI into our economy and society as fast and hard as we possibly can, in order to maximize its gains for economic productivity and human potential.

This is the best way both to offset the *real* AI risks and to ensure that our way of life is not displaced by the much darker Chinese vision.

TABLE OF CONTENTS

What Is To Be Done?

I propose a simple plan:

- Big AI companies should be allowed to build AI as fast and aggressively as they can – but *not* allowed to achieve regulatory capture, *not* allowed to establish a government-protect cartel that is insulated from market competition due to incorrect claims of AI risk. This will maximize the technological and societal payoff from the amazing capabilities of these companies, which are jewels of modern capitalism.
- Startup AI companies should be allowed to build AI as fast and aggressively as *they* can. They should neither confront government-granted protection of big companies, nor should they receive government assistance. They should simply be allowed to compete. If and as startups *don't* succeed, their presence in the market will also continuously motivate big companies to be their best – our economies and societies win either way.
- Open source AI should be allowed to freely proliferate and compete with both big AI companies and startups. There should be no regulatory barriers to open source whatsoever. Even when open source does not beat companies, its widespread availability is a boon to students all over the world who want to learn how to build and use AI to become part of the technological future, and will ensure that AI is available to everyone who can benefit from it no matter who they are or how much money they have.
- To offset the risk of bad people doing bad things with AI, governments working in partnership with the private sector should vigorously engage in each area of potential risk to use AI to maximize society's defensive capabilities. This shouldn't be limited to AI-enabled risks but also more general problems such as malnutrition, disease, and climate. AI can be an incredibly powerful tool for solving problems, and we should embrace it as such.

- To prevent the risk of China achieving global AI dominance, we should use the full power of our private sector, our scientific establishment, and our governments in concert to drive American and Western AI to absolute global dominance, including ultimately inside China itself. We win, they lose.

And that is how we use AI to save the world.

It's time to build.

Legends and Heroes

I close with two simple statements.

The development of AI started in the 1940's, simultaneous with the invention of the computer. The first scientific paper on neural networks – the architecture of the AI we have today – was published in 1943. Entire generations of AI scientists over the last 80 years were born, went to school, worked, and in many cases passed away without seeing the payoff that we are receiving now. They are legends, every one.

Today, growing legions of engineers – many of whom are young and may have had grandparents or even great-grandparents involved in the creation of the ideas behind AI – are working to make AI a reality, against a wall of fear-mongering and doomerism that is attempting to paint them as reckless villains. I do not believe they are reckless or villains. They are heroes, every one. My firm and I are thrilled to back as many of them as we can, and we will stand alongside them and their work 100%.

* * *

June 6, 2023

Related Stories

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

JULY 18, 2023

RESPONSE TO QUESTION SUBMITTED BY MR. KEATING

Mr. WANG. Scale is committed to working with your office, and the Committee to address this critical topic. [See page 10.]

RESPONSE TO QUESTION SUBMITTED BY MR. GAETZ

Mr. WANG. Thank you for that question, and I look forward to working with the Subcommittee and DOD to put in place a comprehensive, risk-based, test and evaluation framework to ensure that AI is safe to deploy. [See page 30.]