CNAS AI TASK FORCE PRESS BRIEFING
15 MARCH 2018

COLE STEVENS,
MEDIA RELATIONS COORDINATOR, CNAS

ROBERT WORK,
SENIOR COUNSELOR FOR DEFENSE, CNAS
AI TASK FORCE CO-CHAIR

AMIR HUSAIN
FOUNDER & CEO, SPARKCOGNITION

PAUL SCHARRE
SENIOR FELLOW, CNAS
EXECUTIVE DIRECTOR, AI TASK FORCE

[*]

COLE STEVENS: Good morning everyone, thank you for joining us. My name is Cole Stevens and I am the Media Relations Coordinator at the Center for a New American Security. We're going to go ahead and dive right in to the briefing.

Today CNAS launched its task force on artificial intelligence and national security. As you're aware, A.I. promises to be one of the most influential and disruptive technologies of the future.

The technology offers incredible opportunities for the world, but also poses serious challenges. The CNAS task force will examine how the United States should respond to the national security challenges posed by the A.I. revolution.

Joining us today are several leaders of the task force.

Robert Work is the former deputy secretary of defense and is now the senior counselor for defense at CNAS. He is the co-chair of the task force.

Amir Husain is the founder and CEO of SparkCognition, an artificial intelligence company based in Austin, Texas. He is a member of the task force.

And Paul Scharre is a senior fellow and director of the technology and national security program at CNAS. He will serve as executive director of the task force.

Before I turn it over to them, I'll quickly address how this briefing will proceed. Due to the large number of callers that we're expecting on the conference line, I'm going to keep all participants on mute on the conference line.

And to keep everything organized, if you have a question that you'd like answered please e-mail it to me. My e-mail is cstevens@cnas.org. I will share those questions in the order that they come in and pose them to the briefers.

To be clear, anything said here can be used on the record. A transcript of this conversation will be available tomorrow for your reference, so please do let me know if you'd like access to that.

So with all that out of the way, I'm go ahead and turn it over to the task force members, who will speak for a few minutes, and then take questions.

So with that, Mr. Scharre, over to you.

PAUL SCHARRE: Thanks. This is Paul Scharre here, for those on the phone line. Thanks, everybody, who's in person and dialing in on the phone.

I thought I'd just start by giving kind of a brief overview of why we wanted to launch this task force, why we think this is significant, and then I'll turn it over to Bob and Amir.

You know, we're at an interesting period of time when we've seen really incredible advances in A.I. and machine learning in the past couple years, and people are beginning to think through what these are going to mean for different parts of society -- in medicine, in transportation, in finance, and in other sectors.

We've seen less of a conversation underway about what this will mean for national security, and I think we're going to see just as significant changes in the national security space as we're seeing in other areas.

About a year ago we launched a new initiative here at CNAS, Artificial Intelligence and Global Security Initiative, a multiyear project looking at how A.I. will affect international security and what the United States needs to do to remain a leader in this space and respond.

Today we're launching a new task force that brings together a diverse array of members -- from former government officials, leaders in private industry, and academic experts in A.I. -- to come together to think about how the United States should approach the national security challenges associated with the rise of artificial intelligence. There are a number of components of this that we're looking to explore as part of this task force.

One is ensuring that the United States remains a global leader in A.I. research and a hub of A.I.-enabled innovation. Other countries have made quite clear that -- that they intend to be a dominant global leader in A.I. We think it's really critical that the United States remains a global leader in this technology area as it continues to advance.

And so that has a lot of important implications for U.S. policy in things like STEM education and other areas to ensure that we're incentivizing innovation and research inside the United States.

Another component of this is empowering the federal government to take advantage of the opportunities presented by artificial intelligence, making sure that the government has the right contracting mechanisms, the right tools at its disposal, the right human capital to tap into this technology where it's happening in U.S. companies because, of course, there are a lot of really amazing U.S. companies that are doing incredible work in this area and want the government to be able to leverage this.

A third area is preparing to counter malicious uses of A.I. technology. We've already seen with very simple uses of things like Twitter bots or homemade drones that both state and non-state actors are using them for malign purposes.

Whether it's Russian use of bots to spread disinformation on Twitter and other platforms, or the Islamic State using small, handmade drones with explosives in Iraq and Syria, we're going to have to be prepared for a world where this technology is very ubiquitous and widely available to others, and we need to anticipate these problems and respond to them.

We also ensure that as the United States uses A.I. for national security applications that it's doing so in a way that is safe, responsible, robust, and transparent; when it's involving things like military applications then of course it's compliant with the laws of armed conflict; and in other areas that might involve things like homeland security, that it's compliant with American values and -- and laws on things like privacy issues.

And lastly, as we're in the midst of this economic transition that will affect a broad set of -- of sectors of the American economy, that we're thinking about national competitiveness and how we, as a nation, weather this period of economic and societal change. When we're looking

at changes in the future of work, that we're doing so in a way that remains -- that ensures the United States remains a global leader more broadly and we remain a society that can weather these challenges.

So with that, I'll turn it over to Bob to give some remarks on how you envision this -- this task force moving forward, and then this issue as a whole.

ROBERT WORK: Well, good morning, to those of you who are here. And good morning to those who are on the line.

I'm really excited to be a co-chair of the task force. The other co-chair is Dr. Moore, from Carnegie Mellon who couldn't be here today.

I'm very, very happy that Amir is here today. I think he's one of the thought leaders in this space, in terms of national security.

And I'm very much looking forward to working with all of the members on the task force.

Now, Paul said, you know, really the task force is about how should the country approach A.I. from a national security perspective. And in my view, the way we have to approach this is whenever you have these big waves of technology that change the society it inevitably will have national security implications.

So the first big wave of the Industrial Revolution had an enormous impact on the way wars were fought. Then came electrification and mechanization, which had an enormous change on the way wars were fought. Then came informationalization, with all of the different types of things that we see today in guided munitions and battle networks, and the informationalization -- everything connected, the Internet of Things.

And I'll use a term that the Chinese use: intelligentization. The next big wave is the intelligentization of our society. And as Paul said, it's going to have enormous impact on transportation, on finance, on medical. And regardless of all of the other things that changes in our society, it will inevitably have a change in the way we must think about national security.

And that's what I'm really excited to work with these really smart people in A.I. over the next 18 months to try to figure out what does it mean for us.

The second thing is, what steps do we have to take to make sure that the United States remains a leader in these technologies? And there are a bundle of technologies when you talk

about artificial intelligence. You talk about advanced computing, like quantum computing or deep neural networks, big data analytics, machine learning.

All of these bundles contribute to the advance of artificial intelligence. It's important that the United States remains a leader in all of these particular technologies.

Now, I have said before and I know several other people have said that this is like the Space Race. I think A.I. is as an important as the Space Race was in the Cold War. And as a nation we responded to the challenge of competing in space.

Key points, but -- but, you know, we created the National Aerospace Agency and we did all sorts of other things as a nation. And so one of the things I'm most interested in talking with the experts on the panel is, how does the United States posture itself for this competition?

Should we have a national A.I. agency? Should we have means by which to attract young men and women to go to college to become coders, to become experts in machine learning, to become experts in advanced computing?

And ensuring the safe and responsible use of A.I. in national security is a big, big deal for the Department of Defense. Paul Scharre was in the Department of Defense and helped write the first DOD policy on lethal autonomous weapons.

And as of this point, we are intent on trying to keep humans in the loop. Some of our competitors may not want to do that. But ensuring the safe and responsible way of using A.I. -- and what that means to us on this panel, at least from my perspective as a former deputy secretary, is will A.I. operate within the strictures (ph) of the laws of armed conflict?

And if it does, that will be a good thing. If any competitors try to use it and not do that, that will be a bad thing.

And then the fourth thing: How do we prepare for the malicious use of A.I.? CNAS just published a really excellent report that I would commend to all of you on some of the things we have to worry about on the way A.I. might be used in a more malign way. And we have to be prepared for that.

So I'm anxious and looking forward to your questions, and I'm very, very honored to be part of this.

And as I said, I'm very, very happy to be joined here by Amir, who I admire a lot. His writings on these issues have inspired me for the last several years.

SCHARRE: Just one quick addendum: The malicious A.I. report Bob mentioned was co-authored with us and many other institutions.

WORK: Oh, sorry.

SCHARRE: Not solo (ph). I want to give credit to everybody else involved.

Amir?

AMIR HUSAIN: Well, thank you very much, Secretary Work and also Paul. It's tremendous to be here and it's tremendous to be a partner with you, and particularly in this endeavor where I think we have to do some very, very important work -- frankly, work of the type that I am not sure exists anywhere else -- in this country, at least, an initiative like this.

You know, my view for a long time has been that "software is eating the world." We thank Mark Andreessen for that quote.

But now A.I. is eating software, and the idea behind that is that even the process of building software is being mechanized. That's how applicable A.I. has become to this whole process of automation.

And what we've seen is that as software eats the world physical things become less important. The differentiation when you build a product, when you build a weapon system, when you build a commercial product, the differentiation that you get by being good at the physical thing has been diminishing over a period of time. The real differentiation has been in the software.

And if A.I. now becomes the way to create that highly differentiated software, then competitive advantage across a whole slew of products can directly be tied to A.I. innovations. The details, of course, are genetic algorithms, and generative techniques, and so on and so forth, but we don't need to get into that.

My point here is simply this: The world is changing in a very specific way, and artificial intelligence broadly applies to competitive differentiation across a slew of different product categories (ph). So I think this is very important not just to our national security but to our economy.

Another thing that I will say is that this is not so much, you know, as they say, the enemy also gets a vote. At the end of the day, when -- when Vladimir Putin says that, look, he who

controls artificial intelligence controls the world, you may take him at face value, you may dismiss him, but then you may see that they're not stopping.

The -- the videos of FEDOR the robot continue to become longer and longer with one, two, three more capabilities added. The speeches, which go from a two-hour speech that now contains 30 minutes of a multimedia presentation showing nuclear weapons being targeted, and -- and -- and Florida is right below them, this is obviously not something that is a question of capability and intent.

And when you look at -- when -- when you look at these statements at face value, the capability appears to be there or is being developed, and by showing these videos we need to maybe re-estimate how serious they are in their intent. It appears to be -- that they're getting to be more serious, so something has to be done there, as well.

So there's a competitive frame, particularly in this new great-power competition era, and it's not something that the U.S. is initiating. There was no speech from the U.S. that showed parts of Russia being nuked delivered by any president of the United States.

The reverse happened. So there has to be some response. There has to be some responsible investment in systems and techniques that can protect against that.

Finally, I will say that America has been the global hub of innovation. We've done a lot of things right, and one of our biggest assets are our universities. These are assets not only because they are all centers of learning and they accumulate so much talent, but also because they are paragons of openness. They are the real doors into America. They are those welcoming avenues that bring people from all parts of the world who want to change the world to America.

And I think as we talk about a lot of the very tangible things, and we talk about a national A.I. policy, and we talk about the Chinese are spending $150 billion, you know, in 2030 and should we spend $175 billion, or hopefully we'll spend more than the $1.2 billion we spend now, but, you know, those are specific things. The bigger things are what will make A.I. American, and in making A.I. American, what will make A.I. win?

There are some fundamental characteristics of the openness, of the freedom, of the exchange, of the multilateralism, of the globalism of bringing in opinions and -- and interests from all over the world to create a technology that is worthwhile. That hardly any other country has the ability to do. That is the superpower that we have right now.

Maybe we cannot outspend the Chinese. But you know what? We've seen an asymmetric fold (ph) is difficult to deal with. That's been our own experience.

It's time I think we start thinking asymmetrically on a lot of these thing -- on a lot of these things. And I think this forum, this group that we're creating today, these kinds of ideas can be voiced. They can be discussed with people with varied backgrounds.

I mean, I know nothing about asymmetry, but Secretary Work knows quite a bit. And so these are the kinds of exchanges that I look forward to in this discussion.

And finally, just to close out, SparkCognition is an A.I. company. We're based in Austin. We focus on three key areas: national security, finance, and industrials and energy.

And in all three of these areas we've had quite a bit of success. We now have over 80 of the largest clients, from Boeing; to Honeywell; to Duke Energy; to NextEra Energy; to Enel, which is the largest utility in Europe; to Flosev (ph); Dover; you name it -- a huge list of clients where we have successfully delivered artificial intelligence technology.

And our work with the DOD is on some fairly advanced topics. One, which is public, is Project Quantum, which is being done with the Air Force to use decision-making -- use A.I. for decision-making. And there are some other projects that I'm not at liberty to get into details of.

But behind us there is Wendy Anderson, who served as Ash Carter's chief of staff. She is our general manager for the defense and national security B.U. (ph). Her team is made up of many veterans: warfighters, people on the front lines, Special Forces guys, Navy pilots -- people that have deep experience of what it means to be able to employ such technologies usefully in the right context.

So at some point we'll have an opportunity to speak with Wendy, as well.

But with this, let me just conclude my remarks and -- and -- and thank the chair, as well as Paul, for this opportunity.

SCHARRE: Thank you, Amir, and thanks for being a partner on this effort.

With that, let's open it up to questions. We'll start first with questions from folks here in attendance, and then open it up to questions coming in over the phone lines.

QUESTION: Yeah. I think the big question from the national security part of this is -- and I know it's something BIU (ph) is working on -- is how do you get Silicon Valley firms to work with DOD when you have things like sharing I.P. and there's, you know, a list of -- of concerns

that they have for working with DOD. And where do you see this going in -- in the short term? I mean, can these companies really be brought in to work on -- on these sensitive projects?

WORK: Well, let me take a swing at this first. This is Bob Work.

I think Mike Griffin was an inspired choice for research and engineering because he comes from NASA, and NASA has a long history of working with the commercial sector to advance U.S. national interests in space. And I believe he's going to come with that very same type of approach to a wide variety of research and engineering, and I know that A.I. is a particular interest right now in the Department of Defense.

In the 1970s and 1980s most of the advances that ultimately led to what we refer to as the Second Offset, which were precision-guided munitions, battle networks, being able to look deep and shoot deep -- generally all those came out of government labs and were pushed by the government. As Amir said and as Paul referred to, there's a vibrant A.I. revolution going on in U.S. industry across the board.

And I am hoping that the United States -- and this is one of the -- my -- as I said, I believe we should have a national A.I. agency, and one of the things that the national A.I. agency should do is to address this problem: How do we address I.P.? How do we address, you know, combining all of the strengths of our DOD labs and our technology sector for the betterment of the country? And this is across all things, you know, in medicine, in finance, in transportation, and yes, hopefully in defense.

QUESTION: And are there some advantages, say, that the Chinese have in that their researchers can move back and forth between classified government work and back into industry without too many impediments or ethical issues or anything like that? With the United States it's a little bit different, right? I mean, people don't move back and forth so quickly and so easily.

HUSAIN: It's not even just the moving back and forth, because information moves back and forth in an instant and a lot of the A.I. research information is available. You can -- you can spend the entire day, you can't catch up with the new A.I. submissions on archive.org. You know, it's -- the information is there.

The issue is that because China is more liberal in allowing large-scale experiments -- and this is a charitable description -- but, for example, if you deploy 5 million cameras in a country and you implement full computer vision and you start to do gesture recognition, and then on top of that you keep layering this complexity and these services to the point where they now basically have a good behavior index, where every citizen, based on their observations, based on their purchase patterns, based on what TV channels they watch and what magazines they might

purchase and where they're found at what times of the day or night, have a reliability score. And that reliability score changes, so an algorithm is somehow determining it with some human seed.

These level of data that you can gather when you've got 5 million cameras deployed and the kinds of objects and situations that you'll see will allow you to build better training systems. So the data advantage, particularly with current deep learning techniques, which are very data-intensive -- the deep learning renaissance over the last few years has been fueled by, yes, better algorithms, yes, better compute, but mainly more data. That they will have a leg up on.

The other thing that I'd like to point out is that there is -- this has happened before. You know, after 9/11 lots of U.S. allies came to the U.S. and said, "You know those predator drones that do such a great job? We need some predator drones." And mostly across the board the U.S. decided not to export that technology to half a dozen different states.

All of those states today have drones. All of those drones are Chinese drones. Some of these states that are our oldest allies are now investing in coproduction plants for those drones.

And it's not just about China got to sell drones. That's not what it's about. It's that now China is in there; now all of the data being produced with those drones is accessible to Chinese experts in multiple theaters all over the world under legitimate cover, and now all of that data is being brought back in figuring out how you improve the product.

That kind of learning -- which, by the way, the U.S. has benefited greatly from that kind of learning. When our allies use our systems we learn from that. That is a data problem.

So I think there is a alternate frame here, which is do you want to deny proliferation? In the military and policy sense the word "proliferation" is a bad word because we immediately think, "Oh, nuclear proliferation," you know, illegal forms of proliferation.

But in the form of the proliferation of smart assets that can capture data and bring that data back to enable the next generation and the next generation of the model to be produced, is that kind of proliferation amongst allies a good thing? If much of the differentiation is coming not from the bended metal but rather from the A.I. model, then perhaps the answer should be yes.

So, I mean, these are fundamental questions. I'm not saying that it -- it must be. It's a discussion point, and I think it's an important one...

WORK: But to your point, let me just follow on. The Chinese have a very unique view on this. It's called civil military fusion, and they really drive the fusion at the national level, which, as a democracy, we would not -- I don't ever imagine something like that.

But how do we in a democracy channel the virtuous fusion of both our commercial industry and our defense industries? And we can approach this. I mean, there are ways to do this.

Andrew Ng, who is the former CEO of Baidu, the way he describes it in -- is in China if someone in the government has an A.I. problem they'll call the commercial sector and the commercial sector will respond. And vise-versa: If someone in their commercial sector has a problem in A.I. they'll call the government and they will respond.

The -- the United States needs to just think through how we do this as a nation, and so I'm anxious to really get down to those type of questions in the task force.

SCHARRE: Amir, I wonder if you had any thoughts on the earlier question about, you know, as the leader of a company that is doing work with both the defense sector but in other sectors, some of the unique challenges in working with the government in the defense space.

HUSAIN: Well, the -- the biggest challenge -- which, you know, this is no revolution; I'm sure all these experienced folks that have been working in this space for a long time know this -- is that for a young company, which, by the way, most innovative companies by definition are young companies because they're bringing some new technology that just came out to market, so that's the case for A.I. companies, as well -- it's just very, very hard to break in. It's very hard to get support. It's very hard to get in on acquisition. It's very hard to get a security clearance done. It's even harder to get a facility security clearance done.

So, I mean, these are really, really slow processes. One example that I'll give you outside of the U.S. context: I was in Brussels just a few months ago and had the pleasure of meeting with the deputy secretary general of NATO, and I'd given a speech on A.I. and hyper war, and at the end he asked me, he said, "What do you think we should do?"

And I said, "Sir, here are all the things we can do for you, but your people tell me that your acquisition cycle is between five and seven years. I live in a world where there is a revolution every 60 days, so seven years is 40 generations. That's such a long period of time that, frankly, I'm not even convinced the universe will be around by then."

So I really don't know what I could do...

WORK: Let me state for the record that I think the universe will be around then.

(LAUGHTER)

HUSAIN: I hope you're right.

So, you know, that -- that to me is the problem. It's sort of, you know, you -- you buy tax (ph) in one way and you've got to buy algorithms in a different way.

We've now started talking in the U.S. military about algorithmic warfare. General Shanahan, as an example, he was there at the last conference that -- that Paul and CNAS organized.

And I still want to understand what does that mean: algorithmic warfare in the context of physical systems and therefore acquisition is still tied to physical systems?

What about certification? Today certification is all or nothing. If you have layers of capability in a system, subsystem software, you certify the whole thing or nothing. There are very old, antiquated ideas.

And so there's some tactical stuff that I've given you examples of, and then there's some higher-level stuff, which is the first frustration that you see in working with it.

"I built this thing. You said you wanted it. Look, it works. Why won't anybody talk to me? Why not -- and who do I talk to?"

And that process for a first-time defense entrepreneur can be ridiculous.

So the other thing I -- I will point out is that we do live in an age where not everybody wants to work with the DOD, and this is just the truth. So those that do want to work with the DOD, I think the DOD should make it simpler for those people to work with them.

SCHARRE: Let me turn to one of you. You manage the Q&A...

STEVENS: Sure. We're going to keep questions for anyone in person, just to keep it simple, if that works. Go ahead and turn it over...

QUESTION: Hi. My name is Gopal Ratnam. I'm a reporter with Congressional Quarterly. Sorry I came in a little bit late.

I wanted to ask you, Secretary Work, you talked about the Space Race and how the analogy here of, you know, mobilizing the country, industry, government together to produce

something similar to that. But the politics of the moment, I mean, there's just, you know, phenomenal change in the last, you know, five years, 10 years, not to speak of 30, 40 years.

What will it take -- I'm just trying to figure out what the challenges are of assembling something even somewhat close or remotely close to a Space Race kind of response, considering that, I mean, back during the Space Race time, I mean, there was no Apple, there was no production of entire components of iPhone (ph) in China. So I want to see what the challenges are of mustering a response like that, and if it's even possible.

And I have a question for Mr. Husain: You talked about what will it -- what will it take to make A.I. American. I wondered if you'd talk a little bit more about that.

HUSAIN: Yeah. I mean that in a spiritual sense. To me, the -- the point is that artificial intelligence has its roots in America, and the kinds of ideas that have developed in artificial intelligence that have taken artificial intelligence in a certain direction are -- are quite American.

In fact, Edsger Dijkstra, who was a professor at U.T. Austin -- and I had great respect for him; he was one of the greatest computer scientists -- but he had the opposite view. He was from Europe, and he wrote a piece that was called "On the Fact That the Atlantic Has Two Sides." And that piece was basically talking about the difference in approaches in America vis-a-vis computer science and the difference of approaches in -- in Europe.

So let me give you some -- something very tangible. Generally if you think about sort of the American way of doing things there's this rapid prototyping Boy Mechanic mentality. I grew up on Boy Mechanic magazines, and Popular Mechanics, and so on, and sort of at some point it's good enough. At Microsoft they say shipping is also a feature. At some point it's done, right?

But there's other cultures and other approaches where perfection is the goal, not getting it done. And in artificial intelligence, actually, it turns out that the internal structure of neural networks and the way that they're being transferred onto silicon is a very -- is very American in its ethos.

What I mean by that is that neural networks appear to not care as much about precision, and if you make neural networks -- in fact, the specific processors that speed up neural networks drop some of the higher-order, more precise mathematical operations to save those transistors and create a larger number of less accurate arithmetic units. And by doing that, by -- by doing something that is less accurate but much larger, so -- so you could, I suppose, call it, you know -- you know, big and fast, you know, big and not-as-accurate -- that approach works really, really well for scaling neural networks.

So, you know, whenever you've been doing something for a long period of time you start to see the parallels, whether it's a poem or a piece of software or a painting or some architectural concept. And I meant it in that sense. There are some fundamental elements of America that one relates to, and one finds those patterns in artificial intelligence -- areas where we've had successes in artificial intelligence.

WORK: It takes leadership from the top. To have a national response you have to have a national push from above.

So it -- in my view it must start from the White House. Perhaps it's OSTP; perhaps it's a special -- a special task force or commission that's put together by the president. But it must -- you must have some type of push from there, especially if you're going to have some type of a national agency.

And it has to be a partnership with Congress. In the Space Race Lyndon B. Johnson was absolutely essential. He said, "Hey, we need, as America, to respond to the challenge in space, and we want to be among the best." And he worked closely with the White House.

So we're going to need something from -- help from Congress, either a caucus or someone who takes this as -- as a leadership position.

And it can be -- the reason why I think it has to be a caucus in this place, just like it was with the Space Race, is because there's going to be an A.I. advocate on the Commerce Committee, and there'll be an A.I. advocate on the Transportation, and A.I. on the Senate and the House Armed Services Committee.

And then there has to be something in DOD. Before I left we recommended -- actually came out of the Defense Innovation Board and said we should have an A.I. center of excellence.

And that actually turns out to be business best practices. I was at a business council meeting in San Francisco where there were 200 or 300 CEOs, and everyone is competing for the same talent in this pool: coders, you know, people who really understand how to put together neural networks, machine learning, et cetera. And what they generally do is have an A.I. center of excellence, which supports all of the business units. And over time the thinking is each of the business units will build up their own A.I. expertise and the centralized center of excellence may go away entirely, or maybe it focuses on moonshots and those.

So I think there has to be leadership from the White House, there has to be leadership in Congress, and there has to be leadership in DOD. And if you get all three of those pulling together then despite the hyper-partisanship that we see, I believe great things can happen.

RATNAM: Wouldn't you know it, though, that there has -- actually it's been more than a year and the White House has not even nominated a science advisor to (inaudible).

WORK: I -- I believe this is an issue, and I'm -- you know, I think the first year -- the way I would -- I interpret this is the first year really was focused on the economics of trade and tax reform, and I'm hopeful that the second year the focus in economics might be on innovation. And we'll see.

HUSAIN: One little factoid about the space program, though: You know, for about a decade it consumed 3 to 4.5 percent of the U.S. budget, and that was the quantum of commitment. In 1966 it went all the way up to 4.5 percent, and that was the quantum of commitment because we wanted to do something great.

That takes guts to be able to go up and say, "This is what I want to do. We may fail," and then to put together one of the world's most miraculously engineering efforts to actually get the darn thing done and to commit 3 to 4.5 percent of the budget over a decade and defend it politically to do that.

WORK: And Amir brings up a great point because one of the things that did, if you listen to Ash Carter, he came aboard -- I think it was called a Schedule D at the time, and Schedule D were for scientists and physicists and engineers, and the new systems analysts at the time. And it drew in an entire generation of what I'll call defense technocrats, who really understood the technology as well as the operations.

We need to draw young men and women into these type of technologies so that we can build up a pool of talent that will serve the nation for decades, just like the Space Race did in terms of talent.

STEVENS: We'll take another question here. Aaron…

QUESTION: Sure. Aaron Mehta, with Defense News. Thank you guys for doing this.

Steven Walker, the -- the head of DARPA now, was asked a couple weeks ago about whether the U.S. is falling behind versus China A.I.

He said no, we're not. We are still ahead. They're catching up, but they're still ahead.

I'd love to get your guys opinion on whether you think that's an accurate read, and if you have a sense of just how far ahead we are at this point.

WORK: Well, let me say this: I never, ever, ever would say -- I would never approach any competition from saying we're ahead. I'd always convince myself, "Man, we're in a tough race. If we aren't behind, we're in danger of falling behind. We have got to fight and we've got to scrap and we've got to go."

This is going to be a world of fast leaders and fast followers. Because all of this technology is readily available to everyone you're not going to get -- I -- I don't think the United States would ever be able to build a two-decade lead in this. It's going to be a tough, tough competition because everyone in the world sees the benefits of A.I.

So I really like Steve. He's a great choice for DARPA. But I would -- I -- what I would ask Steve to do is say, "OK, you may be right, but let's not make a -- let's not even have a chance that you may be wrong. Let's approach this as though we're even. Let's approach it as though we are even-Steven right now and we need to really fight and scrape."

So, you know, saying whether you're ahead or behind right now I don't think is very helpful.

SCHARRE: I agree with that.

HUSAIN: Well, you remember that Eric Schmidt (ph) and I had that discussion -- you were there -- and Eric's (ph) view was five years. I don't necessarily disagree with that if current trends continue.

And current trends being what? If there is difficulty on smart students being brought into the country to work at the best computer science schools we lose talent. If there is -- if there are curbs on their wives being able to come here so that they don't come here because of that, that's a problem. And then if the -- the government funding continues at the level of $1.2 billion, $1.3 billion a year when China is spending $150 billion a year, OK, that's a problem.

The other thing, which I don't know that there's a quick fix for, is that China is able to very rapidly just do things. Five million cameras deployed; data being captured.

Now, that is harder to counter because that's a tangible, real thing. It's not easy, for all the reasons we understand here around the table, to deploy 5 million cameras in the U.S.

So what kind of additional data sets? What kind of other equally valuable data sets can we build that would not be in conflict with our values? So work on that, and research on that,

and, frankly, government funds for that because that's a national asset, these kinds of learning databases.

These are some of the things that we should be doing.

We should also definitely -- Secretary Work has said this a couple of times -- whether through a center of excellence, or a national A.I. center, or whatever we end up calling that, some real government funding. Because, you know, we tend to forget that the cell phones we use, that GPS technology was military-funded, and the cellular network came from the military, and the microprocessor came from the military, and on, and on, and on, and on.

So there has been tremendous commercial benefit from the government and even the DOD spending on these technologies. I think that can happen again.

But there's a long list of things. Current trajectory, if we just continue going the way that we're going, I think five years.

MEHTA: You both mentioned universities at some point in your comments, and yesterday Admiral Hahn (ph) from the Navy was testifying at the Hill and he said, you know, one of the things that we have to deal with is the fact that our universities are centers of learning and excellence that people from other countries are coming to -- China is coming to -- and learning our best practices, and they're able to bring them back.

Is there something that needs to be looked at with that, about whether -- not saying you close things off, but try to figure out how to either, you know, as you said, bring in some foreign capital back into the U.S. and have them stay here as opposed to going back to China, or figure out ways to kind of...restrict that information?

HUSAIN: You know, my (inaudible) view on that -- and in full disclosure, I came to this country as a foreign student, and over the last three years my company has impacted just the Austin ecosystem to a tune over $100 million, all of which is money outside Austin that was brought to Austin because of this company. So -- and I'm, you know, nothing in comparison to many of the other immigrant success stories in this country. So when it works it works pretty well.

Now the question is should we prevent people like that from coming to our universities because we fear that they might heave (ph) something or they might steal something. My view is no.

There are two things that are happening very important to keep an eye on. Number one, the number of Chinese students coming to America is no longer increasing, and I think, if -- if memory serves, it's actually declining. The number of foreign students going to China is continuously increasing. The number of foreign students, non-Chinese, coming to U.S. universities is decreasing. So these are the underlying trends.

You see, when -- when you have a choice now you can go, you can study in the U.K., you can study in Australia, you can study in China, the number one computer science university by U.S. News and World Report is Tsinghua.

So if you want to -- if you have all these options now and now you're also being told, "Oh, you know, we have a problem with your wife and she may not be able to be there with you for X years, and you can't work, and you can't do this, and you can't do that," and the general climate is, you know, these card-carrying Nazis showing up on TV, from the outside it's very -- it's like, what the hell am I getting into, you know? Just get that ticket to China, or whatever -- Australia.

The U.S. wasn't like this. The U.S. was -- I grew up looking at the U.S. through the lens of Archie comics and the Boy Mechanic and Popular Mechanics, and my father and I used to do the projects in the Boy Mechanic, and Radio Shack was like, you know, this -- this heavenly, but sadly doesn't exist anymore. I mean, that was America for me, you know?

And for the kids growing up now around the world America isn't like that. When we talk to them about that it's -- it's actually very hurtful. It's very hurtful to see that kind of change.

But whatever needs to be done to reverse that I think is far more important than trying to curb even more access to our universities. Look, our universities can be responsible. They don't have to provide classified information in undergraduate classes. But in general, the influence that America has had in the world even when these students have gone back to their countries has been tremendous.

WORK: And let me just say as the co-chair -- and I'm -- even though Dr. Moore isn't here today I'm pretty certain he would agree with this -- we're not going to approach this as though we're in an A.I. arms race with China, but without question China is the pacing competitor in A.I. right now. And from a national security perspective that means economic competitiveness, because that will be the wellspring of our ability as a nation to compete in the 21st century, as well as its impact on national security.

But right now China has among the best coders in the world. I actually heard Eric (ph) say he went to the AlphaGo competition thinking we were five years ahead and he came back

thinking that if we were a year ahead we -- we're lucky, and they're closing -- closing fast. The Chinese are closing fast.

And in their own national policy they believe that A.I. is going to increase their economic competitiveness and output by 26 percent. And they are already scheduled to surpass the United States in the size of their economy.

So A.I. is absolutely central from the economic competitiveness of the United States, which, as President Eisenhower always argued, you've got to get the economic competitiveness right before you start worrying about the national security implications of what you want to do.

STEVENS: The next few, if we can keep questions short and answers short as well for the sake of time. Daniel.

QUESTION: Sure. Daniel Cebul, also with Defense News, because we're not great at coordinating.

(LAUGHTER)

So I have two questions. The -- the first is, you know, Eric Schmidt (ph) was speaking at the Munich Security Conference and he sort of nonchalantly said, you know, we're -- we're one to two decades away from, like, you know, an A.I. movie death scenario. So something you've mentioned in a lot of your remarks today is, you know, how do we responsibly develop this sort of technology and what could your task force to ensure that? You know, how much control do we actually have over this technology going forward?

And the second question is, you know, you sort of listed all these things you want to bring together -- industry leaders, and academics, and, you know, thought leaders. What is this task force actually trying to do? Like what is the tangible outcome that you want from this? You know, is this like a product, like a report? You know, what is the sort of overall goal that you guys have?

SCHARRE: Yeah, let me respond to that.

So on the -- the first question, you know, the -- one of the challenges with A.I. technology right now is it is very powerful and already being used in sort of real-world applications, but there are a variety of different vulnerabilities. The systems can be quite brittle (ph), they could learn the wrong thing, they could have biases. We know that many -- some forms of A.I. are vulnerable to spoofing attacks from adversarial data.

So those are the things that we certainly want to think about as the government uses these in national security applications, right? Let's say we're using A.I. to do image recognition to assist in, you know, baggage screening at TSA. If we also know that these image recognition algorithms are vulnerable to spoofing attacks we need to be cognizant of that and factor that into what we're doing, right, and build in those kind of -- kind of safeguards.

To the -- to the broader point, you know, we have laid out kind of for the task force kind of an agenda of ambitious issues we want to tackle. The -- the task force is going to be supportive of our broader research here at CNAS, which will have a series of reports that will roll out later this year, and the task force will help to inform those.

I think it's -- it's a -- it's going to be a little bit TBD and up to the task force members once we get underway in terms of, like, tangible products. Many think -- think tank task forces are not necessarily structured that, you know, you're requiring everyone to sort of sign up to a list of consensus recommendations.

We've intentionally aimed for a really diverse set of members, and we wanted people to be able to, like, have those views and share those views and help inform our research products here at CNAS, so I think we'll -- we'll see, in terms of whether there's, you know, a specific thing that's authored by the task force or not.

WORK: I'm hoping that the task force does ultimately make some recommendations to (inaudible) how do we, as a nation -- how -- how are -- what are some of the things we as a nation should consider to marshal all of the elements of innovation in the United States to make sure that A.I. is a contributor to national security and not a threat to it.

STEVENS: Thank you.

QUESTION: My name's Elias Groll, with the Foreign Policy magazine.

Curious that you've talked (inaudible) how the rubber is meeting the road on these issues for both the U.S. and China. Are you identifying any interesting differences in how the United States and China are applying these technologies in its early stages? Are there different doctrinal approaches with how these technologies are being rolled out now?'

And where do you see the cutting edge right now for both the U.S. military and the Chinese military in how these technologies are being applied in the early stages?

HUSAIN: Well, I'll -- I'll give you my perspective. I'm sure Paul has a lot to add there, as well.

One thing we kind of talked about, right? So China has a completely different regulatory framework, and it's very adaptable because it's the will of a very small number of people that can rapidly change that.

So again, deploying 5,000 cameras with computer vision with no regard for privacy of any kind, allowing police officers to -- to wear caps and augmented reality glasses that have databases of criminals and walk around and being able to identify those, with no worry of whether if one in 100 times you make a false arrest what the implications of that will be. I don't know, but I'm guessing that if that happens they'll say, "Oh, well sorry, you know, move along."

You know, I think it would be far more liability in an environment like this. So those are some very tangible examples of a looser rights framework and just a -- I suppose a different kind of policymaking that enables those experiments.

If you remember during the Bush presidency there was a lot of debate on stem cell research, and stem cell research was banned in the United States. Soon after that China procured massive numbers of sequencing machines and the world's largest genetic sequencing center now exists in China. But not only that, they took that and transformed it into a lead, and this year there were several trials with CRISPER-Cas9 genomic editing on humans in China -- I think over a dozen cases this year -- which isn't happening in the U.S.

My point being that regulation and giving somebody a couple of years to move beyond is a huge deal because then they start to accumulate desk (ph) data; the desk (ph) data informs the next generation, and on and on.

So that's one way in which I see it's different.

The second thing about doctrine, I suppose, is at the highest strategic level China has come out and said, "A.I. is so important that we are going to make it a national priority, and through A.I. we will achieve domination by 2030." The U.S. has not said that. That is a very important distinction.

The third element is that China has already said that they will incorporate artificial intelligence in offensive systems. There is a Chinese modular cruise missile that will contain artificial intelligence systems.

So when you put all of this together and you combine it with the earlier vignette of the Chinese willingness to export technologies such as unmanned drones -- the reason I point to them is that they are great candidates for autonomy. You know, unmanned drones are great

candidates for autonomy with a few sensors and some software fixes added. And you see that happening in the U.S., as well.

So with all of this put together you now have a situation where you have a -- you have a country that's declared that it will dominate via A.I. by a certain timeframe. You see them spending. You don't see them really worrying about regulation, and therefore they have a leg up in being able to test their technologies and gather data much quicker than you. That's how their operationalizing it differently.

And the third thing, you know, again is that from a -- a revenue acquisition and experience acquisition perspective they have no problems bundling this technology and selling it.

SCHARRE: Couple things I want to just kind of add to that, or highlight some of what Amir said: I think the most significant one is that China has -- has made clear that it is a national priority for them, and you haven't seen that from the United States.

It's clear, I think, as -- as Amir pointed out, domestically that they think about the use of A.I. in surveillance in a very different context than we would in the United States, with concerns over privacy.

In terms of proliferation, Amir mentioned sort of armed drones. Look, 90 percent of armed drone transfers abroad come from China. The U.S. has been extremely hesitant to transfer armed drones abroad even to very close allies, and -- and lieu of that China has -- has been the main proliferator of armed drones abroad.

I think that highlights both a difference in how the U.S. and China see related technologies, and that we're likely to see that translate over to A.I., but also the reality that the U.S. does not have a monopoly of these technologies. And in China (inaudible) vote on how they evolve and then how they proliferate.

On the military side there's a great report by a CNAS researcher, Elsa Kania (ph), on Chinese military views on A.I. that goes into a lot of depth. I think at the high level what you see is that when it comes to specific military uses of A.I., like other countries the Chinese military is in the process of trying to figure this out. They do experiments with things like swarming. They try to figure out what you do with some of these things.

There is some amount of -- of mirroring, of doing things because they're seeing the United States or others do that.

I think one issue that in particular is a little bit telling and troubling is the -- the lack of any kind of public statements by China on issues like autonomous weapons implying that they care about the rule of law, or ethics, or responsible use of the technology. I'm just -- very different kind of messaging on the -- on the issue than what you hear from U.S. officials: you know, when he was the Pentagon Deputy Secretary Work talking about this publicly; many times the vice chairman of the Joint Chiefs, General Selva, has spoken on this; the head of DARPA just talked on this a couple weeks ago.

U.S. officials have multiple times publicly said, "You know, we think it's very important to keep humans responsible for the use of force," and we don't hear that same kind of messaging from China. A.I. is obviously much more broader than that, but I see that as a -- a troubling sign.

WORK: The other thing that it seems evident -- and this will become clear as the competition unfolds over time -- that a democracy will try in every way possible to try to keep humans in the loop or on the loop in conjunction with A.I. A autocratic regime, authoritarian regime may not think that way.

The reason why we know that is because in the Soviet Union their conception of what they called the reconnaissance strike complex, which was, you know, machine-generated targeting and guided munitions, was all going to be automated. The whole thing was going to be automated. They were going to try to take humans completely out of the loop.

So it will be interesting to see how the Chinese employ A.I in military scenarios. Are they going to try to be taking humans out of the decision-making loop so they can make faster decisions? Are they going to try to use A.I. to empower humans to make more timely, relevant decisions? And that remains to be seen.

I will say, back to this whole -- and I'm getting a little bit off -- off topic, so I hope Paul doesn't hit me. I believe -- I feel like this is what it feels like to be offset.

In 1996 the Chinese looked at the United States and said, "They are so far ahead of us conventionally that we are going to have to offset their advantages through high technology innovation." And they were very discrete in the technologies they went after: hypersonics, directed energy, electromagnetic railguns, artificial intelligence and autonomy.

And as Amir said, when they say we're going to go after something they really go after it. And I believe we are in the process -- we're going -- you know, we -- unless we respond more aggressively -- and that's why this isn't about an A.I. arms race.

But within my head the Chinese are the pacing competitor, and they are definitely trying to offset our strengths using these types of technologies. And it was -- it's going to require a lot of thinking and a lot of investment to make sure that they do not succeed.

STEVENS: Everyone, it is just past 11:00 so we're going to wrap this briefing up. If you have any questions for task force members after this please touch base with me or get in touch with them directly and we can make that happen.

At this moment any final words from you guys.

WORK: And as I said, I'm looking forward for the next 18 months and looking forward to answering your questions over the next 18 months.

And I ask you to press us and say, "Why are you thinking this?" And, "Have you thought about that?" I would encourage you all, because this is a very important subject.

SCHARRE: Yeah. Thank you all for coming.

And, you know, as -- as other like issues, news items come up in the future, if there's issues you want to reach out to members of the task force, please let us know and we'll -- we'll try to set that.

STEVENS: Again, thanks, everyone, for your participation.

If you'd like to stay up to date with the findings of the task force please make sure that you're on our distribution list. You can e-mail me at cstevens@cnas.org and I'll make sure that you receive everything we put out.

Information on the task force is now also live in the CNAS website. If you go to cnas.org/aitaskforce you'll see updates there, full list of all the members, and any other information.

Again, thank you for your time, and I hope to hear from you soon. Have a good day.

END