THE BROOKINGS INSTITUTION

WEBINAR

REORIENTING NATIONAL SECURITY FOR THE AI ERA

Washington, D.C.

Wednesday, July 29, 2020

Moderator:

JOHN R. ALLEN
President
The Brookings Institution

Discussants:

ERIC SCHMIDT
Chair
National Security Commission on Artificial Intelligence

ROBERT O. WORK
Vice Chair
National Security Commission on Artificial Intelligence

* * * * *

P R O C E E D I N G S

GENERAL ALLEN: Well, ladies and gentlemen, good afternoon. My name is John Allen and I'm the president of the Brookings Institution. It is a great pleasure to welcome you all to today's event, Reorienting National Security for the AI Era. This afternoon's conversation could not be timelier as Congress continues to deliberate the National Defense Authorization Act, the NDAA. Likely to authorize over 700 billion in national security programs, the impending NDAA will undoubtedly make a mark on the future of our country's artificial intelligence infrastructure.

We're pleased to partner with the National Security Commission on Artificial Intelligence, the NSCAI, today. An independent 15-person group, the NSCAI was created by Congress to examine the current AI national security landscape and determine policies that will maintain U.S. leadership in AI research, improve international cooperation, advance shared principles for ethical and responsible use of AI, and related capabilities.

Now this past month, NSCAI submitted its second quarter recommendations to Congress and the executive branch. And we at Brookings are honored and we're delighted to join forces with the NSCAI today to highlight its outstanding work on this topic and to discuss its extensive recommendations from this crucial report.

You know, once considered a figment of science fiction, AI and emerging technologies are poised now to transform our national defense. Imbued with capabilities to change the technology we employ to our war fighters, shift the scope and the speed of the battlefield, and redefine long-held geopolitical norms, AI is and will play a substantial, if not revolutionary role on our national security apparatus. However, as the NSCAI forewarns in their report, the adoption of these technologies is "the work of a generation."

As much as iterative machine learning will take time to strengthen our future AI systems, the actual integration of these technologies into the existing national defense agencies, will also take work and effort. Indeed, democracy may be one of the slowest forms of government, but bureaucracy is easily number two. And only this past February did the Department of Defense adopt its ethical principles for the development of AI capabilities. And further, gaps in talent and digital literacy continue to hinder progress as national security agencies are unable to build the necessary workforce.

Alongside these domestic challenges are everchanging geopolitical landscapes, which also impacts and impedes the future of U.S. leadership in AI technology. Whether used as a means of enacting digital authoritarianism on its citizens, as is evidenced by China, or waging acts of aggression in cyberspace as demonstrated by Russia, AI is becoming the lynchpin of the future great power competition. And moreover, the advent of the COVID-19 pandemic, which continues to rob lives and livelihoods, has also bolstered questions of what the future of U.S. leadership will look like, let alone international cooperation and how it will be, especially as countries turn inward, the focus on this domestic and not foreign policy challenge. One can only wonder what the future of this technology will be in a post-COVID world.

Now, realizing these realities are our two guests today, who are joining us from the NSCAI, Eric Schmidt and Bob Work. Eric Schmidt is known to so many of you. He currently serves as the chairman of the commission and is also a member of the Defense Innovation Advisory Board. He's former chairman and CEO of Google. And Eric has been a crucial leader in the advancement and the development of national security technologies. And it is such a pleasure to have you with us today.

Alongside Eric is his vice chair of the commission, Bob Work. Bob has had a distinguished career in national security for so many decades, having served as the deputy secretary of defense under President Obama and President Trump. And I have to say with great pride, that Bob is also a marine. Bob, welcome and thank you for being with us today.

Let me also note that we were looking forward to hosting Representative Elise Stefanik and Representative Jim Langevin as (inaudible) well, but unfortunately, they're vitally (inaudible) important topics. A quick reminder that we're recording and we're streaming live today. And should you like to ask any questions throughout the event, please feel free to submit them by emailing them to events@brookings.edu or via Twitter at #NatSecAI. That's #NatSecAI. Indeed, some of you have already submitted some excellent questions. We have them and we're very grateful for those. And as time allows, we'll try to get to them all.

Before we get to our discussion, I wanted to start by asking our two guests today, Eric and Bob, for some of their high-level remarks on the NSCAI and then we'll go into the questions. So, Eric, if I may, let me ask you first for some of your thoughts.

MR. SCHMIDT: Well, General, you remember that we started working with you all a couple of years ago when you got interested in the bipartisan issues of AI and national security. I can tell you that Brookings is the perfect place for us to have this conversation. And under your leadership and the staff you've assembled, we're going to see a big impact from the Brookings work in this area as well. I'd also like to mention that Secretary Work and I are speaking in our respective capacities as chairman and vice chairman of the NSCAI, and not in our other various hats that we have.

You know, over the last three months, we worked to develop recommendations that we believe address the geopolitical, economic, ideological, technological, and military challenges that we're confronted with today. As you mentioned, General, AI and its associated technologies are central to meeting the demands of these challenges and will help the United States navigate today's turmoil, right, which is sort of ongoing and constant, I think, in the world today, to make it essentially a more secure future. Which is what we really care about.

The consensus that we have developed over the last year and a half in our commission, which I'm very, very happy to be a member of, is that the United States government has to organize, resource, and train to understand, develop, and deploy these AI technologies. It is a national priority. It is an urgent matter and I don't accept the answer, oh, it's the bureaucracy and it takes a while and so forth. We need stronger leadership. We have that in some members in Congress such as the ones that you mentioned. We have it from you. We need it from everybody else.

And by the way, we need to do this stuff ethically, responsibly, and in partnership with the private sector and academia because much of the actual research is being done there. It's not being done in the government. So, the government and the private sector have to figure out this partnership. And we talk about that in our report.

So, what we're trying to do is we're trying to imagine a future that has not arrived yet. And so, we are forecasting what will be true and we're trying to get the private sector or the companies and the government ready for it. And I want to emphasize and I know Bob will emphasize this three times more than I, that this is a lot about talent and it’s a lot about people and it's a lot about focus, right? And I know that sounds boring, but in fact, it's true, right? It is fundamentally a human problem.

So, from my perspective, we need to have an expansive view of promoting AI leadership.

We're trying to separate hype from reality. We're trying to make sure that these AI developments progress in tandem with a larger reorientation of national security to compete in this new world of what is now called in the General's world, strategic competition. It's no longer us and then these little guys. It's now real strategic competition and I want America to win, right? And I know you guys do as well. So, in our case, many of these ideas in the commission that are developing will require consensus, and it will take some consensus building. And what I am sure of is that Brookings and the people who are watching our show today will help us in forging that consensus. I can think of no higher priority for the nation once the pandemic is behind us. Secretary Work?

MR. WORK: Thanks, Eric, and thank you, John. I just want to echo Eric's thanks to you and to Brookings for hosting this this afternoon. You know, on July 20th, the reason we're here this afternoon, is the commission voted on 35 discreet second quarter recommendations to both the legislative branch and the executive branch in six areas. Now, this follows 43 recommendations from our first quarter report. Generally, the way you should think about it is our first quarter was really focused on trying to do low hanging fruit. To exploit things that were already easily exploitable. And in this quarter, we started to talk about bigger ideas. We'll follow this up in the third quarter and as soon as the third quarter recommendations are done, we'll turn our attention to the final report, which as Eric said, is due in March 2021.

So, we have these six lines of effort that I told you about. Actually, we have seven, and I'll talk about the seventh and just very quickly. But the first is invest. And so that is advancing the federal government's and the Department of Defense's internal AI research development capabilities to ensure that we maintain the edge in a global strategic competition in this new emerging technology.

The second line of effort is called apply. And it is really focused on accelerating AI applications, which is how, John, as you said, we'll really start to see the changes in the bureaucracy in the government, in operations, in intelligence, the applications are very important. And so, what we're trying to do is identify, prioritize, and resource the infrastructure necessary to get those applications to the field as quickly as possible.

The third area is under the rubric of training. And as Eric said, this really is about getting our AI talent to the point where the digital and AI literacy of the entire federal government and the

Department of Defense and the Department of Energy is world class, and we have the people that can really drive the changes that we are all hoping to see.

Line of effort four is called protect. And this is about protecting our AI advantages for national security through discriminant use of export controls and investment screening. We have to protect our national security's sensitive elements of AI and other critical emerging technologies from foreign competitors. But we need to do this in a way that doesn't undercut our own competitiveness and our own innovation.

Line of effort five is marshal. This is focused on the Department of State. Competitive diplomacy in AI and emerging technology is a strategic imperative in an era of great power competition. And our allies and partners have a lot to offer here. And we want to be able to have a means by which to marshal these capabilities.

The sixth area, as Eric said, the commission is convinced that we have to be able to do this in an ethical way, responsible way, with close-end partnerships with private sector, academia, and non-government organizations, and our international partners. So we have an entire line of effort on creating a framework for ethical and responsible development and fielding of AI. And what we are focusing on is it's one thing to publish these principles if many of the organizations don't know how to apply them. So, we spend a lot of time trying to think through how organizations could actually apply ethics in a way that further their own mission, as well as the broader mission that we're trying to accomplish.

I mentioned we have a seventh LOE. That's a classified LOE and it's focused on trying to understand what our competitors are doing in this space so that we can anticipate vulnerabilities, et cetera.

Now, we're working towards our final report in March 2021. We're going to continue to solicit feedback from a diverse range of experts in the field, non-government organizations, businesses, scientists, government officials, organizations like Brookings, and work closely with our partners in the executive and legislative branches. I know Eric would agree with me that Congress has been phenomenal in their support for this Commission. We consider them to be our primary customers. And as you said, Representative Langevin and Representative Stefanik who are on the intelligence, emerging

tech and capabilities subcommittee of the House Armed Services Committee, they have been true champions. And we're sorry they couldn't come today, but I think everybody understands they were pulled away for pressing business on the Hill.

We really look forward to your questions this afternoon. And we look forward to questions after this event. So, with that I'll turn it back over to you, John.

GENERAL ALLEN: Thank you, Bob. Eric and Bob, thanks very much for those opening remarks. And, Eric, thank you for the confidence that the commission has that Brookings can help you in the work, but also help to continue the work as time goes on. And, Bob, thank you for laying out those lines of effort. It certainly is expansive. It certainly offers a lot of very important opportunities and challenges. And I think we should all be grateful to the Congress for its wisdom and its insights in being able to see the importance of this commission at this particular moment.

Let me transition to the questions. And I'm very sorry we don't have a lot of time today, much more time than we've been able to allot. But I think we have the opportunity to answer some very important questions. And this report has such rich content. And as both Eric and Bob, you said, we are challenged in many respects by an absence of talent. Not an absence of capability, but we've got to develop the human force necessary to back-up the work that we will do.

And so to that extent, if I could, Eric, if I could impose on you, please, to give us your thoughts on one of the innovations out of this report, which is something called the U.S. Digital Services Academy, the USDSA. And what you would hope to see and accomplish, and perhaps in the context of how we have viewed academies in the past. I'm a graduate of the Naval Academy. How would this USDSA serve the greater needs of the United States? And then, Bob, let me ask you after Eric's done, to talk about another great innovation I think coming out of this report, which is the National Reserve Digital Corps. Both of these are fascinating and I think we'd all benefit from hearing your views on it. So, Eric, if I could ask you first?

MR. SCHMIDT: Thank you. This actually started between a conversation with Bob and myself and some of our military members of the panel. And, you know, my observation was that the academies have served our nation well. And it turns out the academies are producing technical military people and list, you know, basically officers. There is no equivalent on the civilian side. And yet the need

is probably greater on the civilian side because as both Bob and John know, the vast majority of the stuff is done by civilians who are under contract to the military and to the various basically information agencies of one kind or another.

And so, we made what I consider to be a very modest proposal, which is to start a digital service academy largely around civilians. And we make the argument that when you look at the cost of developing talent and so forth, that this is actually cost-neural to cost-positive, right? In other words, that this is not an extra huge line of expense. And Bob then came back and said, well, we like ROTC, which I certainly favor very strongly. I think it's very important for our nation's strength. So, Bob came back and said, well, let's talk about something analogous to ROTC, which he named the National Reserve Digital Corps. Bob?

MR. WORK: Yes, and just a little bit more, John, on this. You know, there have been talks of U.S. public service academies for some time. In 2007, there was actually a group, a bipartisan group of senators who sponsored legislation to create this academy because we wanted to draw in young men and women citizens into our government. A large proportion of the government service force is reaching retirement age. And so, we know that we need to be bringing in young men and women to feed, you know, to grow a new generation of government servants.

But we also want to bring in a lot of STEM talent. So, the whole purpose of this idea is to say, well, let's have one category, the U.S. Digital Service Academy, which would bring in folks that want to serve in government as a career. So, when they graduate, they would be a GS-7 we anticipate on a GS-7 911 track. And they would be, you know, it's competitive promotions thereafter. But they're coming in they know they want to try a service in the government.

National Reserve Digital Corps, as Eric said, is based upon the NROTC and in effect, they would be our reserves. And they would graduate and they would have a commitment of five years. And during that five years, they would agree to work for 38 days a year, just like the national guard. Two days a month they would go to some type of agency or some type of military unit. And what they would do is I am here to help you think through how AI enabled technologies will help you accomplish your mission. And then for 14 days out of the year, they would go to a major joint exercise or a war game. And they would do the same thing. They would watch and listen and learn the problems and try to figure

out how AI-enabled technologies would help them.

Now, remember this follows on the heels of the first quarter recommendations. And the first quarter recommendations were saying, look, we think we have a lot of talent inside the military that we just aren't aware of. So, one of the things that we recommended was we would actually try to grade, you know, we would have like a programming proficiency test, like a language proficiency test.

GENERAL ALLEN: Mm-hmm.

MR. WORK: So, we could identify all of the young men and women who serve in the government or the military and who have talent that we could then draw upon. The other thing we talked about was adding a computational thinking component to the armed services vocational aptitude battery so that we would know the talent of people coming in. So, it's all of these things together, John, that the commission was looking at to try to increase the digital literacy and talent of the U.S. government and military so that we are a world class AI organization.

GENERAL ALLEN: Well, those are fascinating ideas. And as you say, Bob, and I think we all have recognized from our time both in and around the services, there's a lot of talent in the ranks of our services that we just don't know about. And we've learned about that in the -- you used the analogy of the language aptitude tests that we've been giving for years. We have lots of troops that have real language aptitude. My guess is we have a tremendous amount of digital aptitude in our ranks that we just don't know about. So, that's a tremendous innovation, but I think the academy is a great way to go. We've been thinking about those national security type academies for a long time, above a service academy. But even more important to all of the agencies, which is what this feeder would do, but also the reserve corps gives us some depth in a moment of --

MR. WORK: Yeah.

GENERAL ALLEN: -- an emergency and keeps them current. They're just brilliant ideas.

MR. SCHMIDT: So, John, let me add --

GENERAL ALLEN: Sure.

MR. SCHMIDT: Let me just add one -- let me add one more point. So, the canonical view is that the government cannot hire these people because they'll get paid more in private industry. My experience is the inverse. My experience is that people are patriotic. And that you have a large

number of people. And this, I think, is missed in the dialog. There's a very large number of people who want to serve the country that they love.

GENERAL ALLEN: That's right.

MR. SCHMIDT: And the reason they're not doing it is there's no program that makes sense to them. So, I suspect that if we can convince the Congress to make this real and the President signs off, hopefully, then not only we'll be successful, but we'll discover that we need 10 times more. The people are there. The talent is available, right? This is a fitness problem. It's not a I'm not motivated. If there's anything I've learned in working with the government and I know this is true of Bob and you, is people are patriotic. They really care. They want to serve.

GENERAL ALLEN: Eric, you and Bob have (inaudible), I think, a wonderful idea. And I hope the Congress is aggressive in following through on it because it's both the time and it's the idea.

Let me shift a little bit in the questioning now. As you both are so intimately aware, as we embark on an era of artificial intelligence and related technologies, ethics and fairness could not be more important. And as we seek to harness AI for good, we need to be mindful that it can also pose some significant risks in the context of perpetuating ethnic or racial bias. So, Eric, let me just ask if I could, how is the NSCAI thinking about ethics and fairness in the context of your deliberation? And then, Bob, I'll ask you about how we'll seek to harness and harvest the great strength that is available to us in this country through our diversity?

MR. SCHMIDT: Well, you said it very well. And the problem with AI is that the data can be biased and it's also as a technical matter true that some of the implementation choices can have an unintended bias. That is literally the way the code works. So, you can have both bad data and also the algorithmic choices can introduce bias that was unintended. And most organizations, including the Pentagon, have now adopted ethics principles, but they're typically very broad in language, and, frankly, it takes quite a bit of training and understanding. So, we had the idea and one of our commissioners, Eric Horvitz, did much of the initial work along with our support, was to try to write a paradigm for how you would operationalize these ethical AI principles. And so, we recommend specifically that the national security agencies implement the paradigm that we've laid out in our document. The document's public. So, everyone watching this, take a minute and read it and does it make sense to you?

And we also sort of are insisting that these users develop processes and programs that implement the practices and monitor their implementation and continually refine them. So, we're trying to move the ethics conversation to an implementation, not just a wish. Bob?

MR. WORK: Yes, I mean, one of the things we did, John, in our initial report was to explain that the strategic competition was also a competition of values. Values are reflected in the artificial intelligence applications and the way they are applied. And woe to all of us if the Chinese view of AI and the values propagate throughout the world. I just happened to see today in the Atlantic, there's a new article out. I haven't had a chance to read it, but it's called, China is what Orwell Feared. And its subtitle is, *AI Enhances Totalitarian Control and China is now Exporting it*. So, they're not just exporting technology, they're exporting values. And it is important all of the commissioners are absolutely rock solid behind the idea that we need to maintain our values and our ethics and our morals in the applications of these AI. How do we protect personal information? How do we avoid using this type of technology to enhance governmental control of populations?

So, I mean, the commissions talk about this all the time. And has Eric said, Eric Horvitz has really helped us think through. He's passionate about this idea and he said we have to start to inculcate this idea throughout the government, which is what Eric was saying. We're trying to give them a template on how to actually implement these ethics.

Now, we believe that we can do both in parallel. That we can continue to innovate as we debate ethics and debate the limitations of the technologies. And this is something that all of the government, every single cabinet department and chief technology officer and chief data officer has to be aware of. And so, this is often one of those things, well, tell me how AI is going to help me kill that tank over the hill. The first question you have to ask is, okay, yeah, AI can help you kill the tank over the hill, but how can it help us avoid non-combatant casualties?

GENERAL ALLEN: Right.

MR. WORK: How can it help us avoid collateral damage? Because AI can do that too. So, we're confident we can do this in parallel.

GENERAL ALLEN: Well, it's extraordinarily important point. And I think one of the great differences between us and the other side will be if as we consider the implications and the application of

these technologies, if we just take a step back and consider first principles, and those first principles being our values, then that will guide us forward in the right direction. And that's such a powerful outcome of the Commission is constantly honing-in on that issue of values.

So, let's talk a little bit about some of our opponents. The United States and its allies are by no means alone in looking to develop advanced technologies. And China and Russia and other rival powers are seeking to create cutting edge capabilities that not only have application on the battlefield, have application in strategic influence operations, but also sadly, and too often that technology is used to repress the rights of minorities and other human rights dissidence.

Now, the NSCAI it highlights a number of ways to counter that threat, including export controls. And, Eric, if I could ask you, could you talk a little bit about how you see these controls and how do we -- because this is difficult, AI often the algorithms appear to have dual-use values. How do we implement these export controls in a targeted way?

MR. SCHMIDT: Well, first place, let me give you a sort of conceptual framework that I have been operating under. And you might think that with artificial intelligence and national security you could create a Los Alamos that would create, because Americans are so incredibly smart, some kind of special military advantage. I, and I think the Commission, have come to the conclusion that the technology knowledge around algorithms and software is so diffuse. In other words, it's so spread that if you were to do the Los Alamos model, there would be an equivalent group somewhere else that was doing the same thing. In other words, the notion of secrecy is not going to get you where you need to go, at least on its own. So, that's observation number one.

We talked at some length about software versus hardware and there is an emerging consensus among the commission that there are more likely to be hardware things that should be protected than software, sort of as a comment. And so, what we concluded was that we needed a more sort of thoughtful and strategic framework for how these things would work. How CFIUS would work. In other words, if you just ban everything, all you're going to do is hurt Americans. And if you just say yes to everything, all you're going to do is hurt Americans, right? So, you have to find that sort of strategic coordinated and sort of rigorous. So, we basically give a set of principles in the document for specifically around how the controls work.

And I want to say right now, that if you're using control to try to get competitive advantage, you're losing. Control is not a supplement -- sorry, a replacement for innovation, right? You have to innovate and if you can control, that's great too. But control itself, because the technology is moving so quickly, won't hold it. And I think that exports are -- these controls are difficult to apply to AI and that they have to be judiciously applied to each part of the stack, and we take the reader which parts. And the stack includes hardware and various forms of specialized code and specialized processor algorithms and then thinking algorithms and then applications algorithms and the use of data.

And we do conclude that CFIUS needs to be more heavily utilized to prevent malicious investments. So, we do think that being wary is the correct attitude. Bob, did I summarize that to your satisfaction?

MR. WORK: Absolutely. Just want to foot stomp, John, what Eric said that we concluded that controls on software are very, very difficult and would actually undercut our own competitiveness. So, but export controls on hardware, there is a lot of room there that might be an advantage to us in a long term competition. But what we have to do is we have to split apart export controls from investment screening. So, right now CFIUS only is worried about technologies that are on the export control list. But there's a whole other list under ECRA, the Economic Control and Reform Act, which are called foundational technologies. And a lot of these are something that CFIUS needs to be following too. So, in addition to splitting software from hardware, we also recommended splitting investment screening from export controls.

And the last thing is, man, we've got, you know, we have five allies that we share our most sensitive intelligence with and they have to go through the whole CFIUS process just like somebody who's not an ally.

GENERAL ALLEN: Right.

MR. WORK: And it just doesn't make any sense to us. So, the other thing we recommended that we wanted to have a fast-track for our allies in this (inaudible) process because our whole LOE on marshal coordination and collaboration around the world is very, very important in a global competition for values. And we would like democratic values, obviously, to rise to the top and be generally the benchmark for AI-enabled technologies.

GENERAL ALLEN: That's right. We can't be our own self-limiting resource --

MR. WORK: Yes.

GENERAL ALLEN: -- in this regard. So, very, very, important.

Interesting part of the report talks about the State Department. And, of course, you know, the leading edge of American influence, while 10 carrier strike groups is pretty impressive, the leading edge of American influence are our magnificent diplomats and our ambassadors and our State Department employees who live in harms way every single day around the world at our embassies in our consulates. State Department, in particular, is going to need to become much more adept at the integrating this technology into U.S. foreign policy. Bob, let me ask you, you had some recommendations in that regard. Can you give us some thoughts on that? And, Eric, could you come in behind Bob and talk about how state and defense could be coordinating as they go forward, please? Bob?

MR. WORK: Yeah, John, this is really, really important. The --

GENERAL ALLEN: Bob, we're having a little bit of trouble hearing you, please.

MR. WORK: Okay. I'll get closer.

GENERAL ALLEN: Thank you, sir.

MR. WORK: State Department really needs to consider the technology competition as an absolute pillar of our global strategy in a long term strategic competition with authoritarian powers. Can you hear me, John?

GENERAL ALLEN: I got a live microphone.

MR. WORK: Is it good?

GENERAL ALLEN: Good, please.

MR. WORK: Okay. So, there's already an idea to have a bureau of cyberspace security and emerging technologies in the Department of State. That came from the Department of State, but it stalled for whatever reason. We're not really certain. And we said, look, let's clear away the impediments and get that into place because that could become the nucleus for the strategy and the talent within the Department of State to actually think about how we would do this in a more broad way.

We also recommended establishing a strategic innovation and technology council composed of the Department of State's senior leadership. And, you know, this type of stuff, this big

change, as you know, John, has to come from a top down. It can't bubble up. If we want to have transformational change and really start to gain momentum, it's got to come from the top. So, we thought a strategic innovation and technology council leaning on the cyberspace security and emerging technologies, or CSET Bureau, was the way to really get the state going. We recommended AI training in all of the FSO, the Foreign Service Officer training. We recommended having a technology officer in each of our embassies and consulates. We have to make technology more central to the way diplomats think about competing in the world and spreading American and democratic values.

GENERAL ALLEN: That's terrific. And, Eric, how do we get defense and state to coordinate on these?

MR. SCHMIDT: Well, it's interesting, as a follow-up to what Bob was saying, the State Department actually has a chief technical officer who's a friend of mine, Mung Chiang, who is brilliant. And the DOD has created this thing called the Joint Center for AI, JAIC.

GENERAL ALLEN: Mm-hmm.

MR. SCHMIDT: Which is having a transformational impact starting with imaging. So, it seems to me that that's a natural pairing to start with. And one of the things that we recommend, by the way, is in addition to the obvious pairing, which would be done between the two groups, that the Congress should hold hearings to make sure it's actually happening.

GENERAL ALLEN: That's very good. Let me just -- this will be the last question I'll ask you and then I'll go to some of the questions that have been given us by the audience. You won't be surprised to learn it's about China and the Xi Jinping regime has been unambiguous on its AI ambitions and its intent to develop advanced technologies. As we watch this unfolding and as we watch the very clear deterioration of relations between the United States and China, what are your views, if I could, Eric, on how seriously we should take China's ambitions with respect to artificial intelligence and emerging technologies? And how will the NSCAI's recommendations position us to meet the challenges posed by China? And then, Bob, let me ask you to come in behind Eric by answering the question that the U.K. has recently joined the U.S. in banning Huawei from its core telecommunications infrastructure. Could the U.S. and the United Kingdom continue pressing other democracies to adopt similar measures? Eric, please?

MR. SCHMIDT: I was in China right before the COVID crisis. And I became quite alarmed that China has managed to simultaneously solve the problem of identity in the form of face recognition, e-commerce in the form of their billing system, mobile phone, and convenience. And that integrated system provides value to the Chinese citizen and also value to the state in terms of surveillance. If you simply extrapolate from that system and you take China at its word that they want to dominate AI by the year 2030, you could imagine a system which is both brilliantly powerful and brilliantly constraining invented by the enormous investment that they are proposing and indeed making.

We need an answer. And our answer is in the outline of the report that we've given. It starts with partners. It starts with talent. It starts with focus. And it starts with values. You combine all of those together to have an alternative. We have no choice. The game is afoot. It's happening. And people say, oh, that' fine. That's going to happen in the future. China's not very good. All of these things are false, right? China is now the leader in key categories. And I'm concerned that we maintain our leadership in the key categories we're already doing and compete with them in the ones where they're leading. The game is afoot. The competition's ahead of us. We need to take it seriously and we need to act now. Bob?

MR. WORK: Yes, I can't agree more with what Eric said. And what our citizens and our representatives and senators and government leaders have to understand is this competition is much different than the Cold War. You know, the Soviet Union could compete in niche technological areas like nuclear weapons and space. But we just clean their clock in the broad panoply of emerging technology and digital microprocessors, information systems, et cetera. But as Eric said, China is our technological peer. And it will be ahead in some areas and we'll be ahead in some areas. But we're both going to be pressing each other like crazy.

So, you know, in this type of competition, I'm always reminded of the old political saying is, always run a race like you're losing. And I think it's just more important to do that with China in the technological and AI competition than anything. Now, one of the advantages of being the vice chairman, is I can defer to the chairman on questions like what about Huawei? Eric has been working extremely closely, has been speaking to people in government in the executive branch, in the legislative branch, and our allies. So, if Eric doesn't mind, I'd like to toss that ball back over to him because I think he would

be able to give a much more cogent and insightful answer than I could.

GENERAL ALLEN: Mr. Chairman?

MR. SCHMIDT: Thank you, Bob, and I'll return the favor. So, a little bit of the background on 5G is that we over the last decade have had a poor strategy with respect to 5G. We did not make available the right amount of frequencies in the right places for the telecom industry. We also allowed the majority of the industry to become outside a nondomestic industry. We essentially lost both the race in terms of spectrum, as well as the equipment suppliers and some of the technology base. That was a very strategic error because 5G is crucial to where we are as a society going to go and also how the military will work. So, it turns out that the asynchrony and the synchrony of 5G allows for much tighter integration of autonomous systems. Something which is crucial, for example, for national security issues, without getting into the details. You can imagine what they are.

So, it just seems like this was a policy failure throughout the country. There are a number of solutions, but at the moment, we're sort of playing a catchup game. We're saying don't use Huawei because there's evidence of Huawei's misuse, if you will. And there's a broad consensus that Huawei can be misused by the Chinese government and others.

But we don't have a strong alternative. There's a number of proposals floating around of how to do that. I'm strongly in favor of getting more frequency available to the domestic suppliers. And if you're confused about that, think about how slow your phone is and then image that you want a phone that's a gigabit phone. And 5G has the technical capability of delivering that to 80 or 90 percent of Americans. And it can be done in a relatively small number of years and it can be done economically. So, that's why this is such a big deal.

GENERAL ALLEN: Thanks for that elaboration. I think an awful lot of folks just don't have that kind of detail, and that's fairly important for us to have. Let me, if I may, we've just got a few minutes left. I'd like to go to some questions from the audience. Eric, could I ask, please, because it's on everyone's mind every day, how has COVID impacted the NSCAI and its policy recommendations?

MR. SCHMIDT: Well, frankly, we just went virtual like everybody else. And I think that we're important, but COVID's even more important. I am worried that the government collectively its response has been less than optimal. And that there are plenty of examples where AI has helped in the

research and so forth for cures to COVID. So, for example, virtually all of the interesting RNA modeling is being done on AI platforms. Almost all of the interesting drug discovery is being used on AI platforms. But, frankly, we just need to get this thing over. An awful lot of people are being harmed.

GENERAL ALLEN: Bob, have you seen as you've looked out across the waterfront, so to speak, countries, other countries than the United States using AI or effecting AI policies that have been helpful in flattening the curve with respect to COVID?

MR. SCHMIDT: Well, in a negative context, the Chinese strategy, which was essentially a forced app, and then the use of machine learning and data to violate your privacy to figure out who you had in contact with to essentially enforce contact tracing worked. I am not advocating that for America. I think it's a violation of our values. But we have not tried, in America, to do things using AI at scale that preserve our values. So, we are again, not innovating in this area.

GENERAL ALLEN: Bob, any thoughts?

MR. WORK: No, I can't add anything to that.

GENERAL ALLEN: Let me go to a second question. This is obviously a national security commission and there's a lot of conversation about how AI will affect warfare as we go forward. And so, Bob, let me ask you, and, Eric, please come in. We've talked about the integrational issue that it's going to require long term integration of capabilities, but is there as you think this through, a definitive effect that AI will have on both conventional warfare and very importantly, and we've talked about this in other conversations we're having, the potential for nuclear warfare?

MR. WORK: Well, I think we are learning as we go, but our hypothesis is that the widespread injection of AI-enabled applications and autonomy into U.S. combat control systems, command and control systems, all of these things will lead to something that we refer to as algorithmic warfare. It won't change the nature of war, but it will change the character of war where algorithmic competition becomes central to the military competition. And the side that has the best algorithms and employs them in the most innovative manner to gain advantage on the battlefield is really going to have an enormous advantage.

Now, we started with, as Eric said, Project Maven, which was all about how do we exploit computer vision to help analysts understand the tsunami of information that just crashes over them every

minute, every hour. And most of our analysts and a lot of our operators spend a lot of time staring at a computer screen. And it is just a total waste of their talent. We should let the computer stare at the screen, pick out the information that the analyst needs to know, and act upon. And then you take that to operational planning where AI might be able to come up with recommendations for courses of action and provide analysis of plans. And what we think algorithmic warfare will do is speed everything up.

In fact, you have written on this, John, with Amir Husain from SparkCognition, and you refer to it as hyper-war. And we see it very much the same way where we will understand the battle space quicker. We will be able to make better decisions faster. We'll be able to apply more discriminate effects more rapidly. And so, the entire operations start to speed up. And, you know, the way we train our commanders to handle this type of algorithmic warfare is going to be very, very, very critical.

So, the thing we're trying not to do is overhype AI. But we're confident that it is going to have an enormous impact at the strategic level and the operational level. A lot of people are worried about AI. This is me talking now, not for the Commission. But for example, the thing that I worry about most is an artificial intelligent machine that could order independently either a preemptive or retaliatory strike.

GENERAL ALLEN: Right.

MR. WORK: I believe that would be extraordinarily destabilizing at the strategic level. And there are going to be things like that that Eric talks about all the time that we will want to talk with our competitors about.

GENERAL ALLEN: That's right.

MR. WORK: And say are there things that we should avoid in the interests of both of our countries? Because AI will be able to do that, but it isn't an application that we would really want to pursue.

GENERAL ALLEN: Eric, any thoughts?

MR. SCHMIDT: Yes, and let me just speak for myself, so and just as a person. I completely agree with the way Bob described this as algorithmic warfare. And when a new form of warfare is invented, there will be new tactics. And one of the new tactics will be one of the first things you'll try to do in such a scenario is you'll try to attack the other folk's algorithms.

GENERAL ALLEN: Right.

MR. SCHMIDT: So, you have the situation where if you have an automatic weapons system, which Bob and I are very concerned about, you could imagine a situation where that attack could become part of the doctrine of how the war would go on. We have no language, we have no way of conceptualizing that. So, you combine the fact that the system that's making the decision could itself be attacked, right, in a war act. And the compression of time to the point where the what is known as the OODA loop, right? Which you know well, which is the cycle of observe and detect and act, is thought through can get so short that it affects -- it's faster than what humans can decide. And so you get a situation where you have a single individual who has to make a split-second decision based on possibly false information. And that is an inherently destabilizing problem in a sort of stable world order.

I think, speaking personally, the best way to deal with this is to begin diplomatic conversations about these issues because they affect not just the United States and China, but Russia and other countries as well. Because we're not going to be able to prevent this technology to eventually be at least theoretically possible for countries and also terrorist organizations. And we don't want this scenario in front of us.

GENERAL ALLEN: Well, Bob, you mentioned it, and Eric, you expounded on it that the whole idea of the acceleration of warfare. And it goes back to the original thoughts that we had on the digital service academy, national reserve digital corps, or the national reserve capabilities that we may have. And I think the advent of artificial intelligence and the digitization or the algorithmic approach to warfare is going to require a different kind of talent. And it's going to also require not just a different kind of talent, but also a different kind of education and training.

Now, one of the challenges we had, I had the honor a couple of years ago of leading a study for a think tank in Europe called GLOBSEC, where we looked at how NATO will be adapting to the future environment. And one of the things that we concluded was while there will be real challenges for NATO, and this is part of a question that we've gotten from the audience, one of the greatest challenges that NATO will have isn't going to come necessarily from opponents. It's going to come from a widening of capability technologically and a gap that will emerge between the United States and our allies. So, how do we think about this now? How does the United States really lead, not just with NATO, but the

whole community of democracies around the world, how does the United States really lead in NATO, but also with its allies around the world in not just the technology of AI, but lead in the ethical application of it? And I think this will probably be our last question. So, please, both of you, this is a great opportunity to finish up on values.

MR. SCHMIDT: Bob, why don't you start?

MR. WORK: Well, the key thing in this is because each country has its own kind of moral and ethical frame, this is not something that the United States can dictate to its allies. This has got to be developed and collaborated with our allies. You know, Eric and I used to joke that, yeah, right now we have the five eyes, like eyeballs. And they're our closest allies. But what we really want is about 50 eyes, AIs. And we want us all working together, democracies. We want our values, all of our values to be manifested in whatever we do.

And this can't be somebody dictating because everyone will have a slightly different moral and ethical frame and we will have to debate these issues and they're going to be contentious. We see this right now in the U.N. Council on Conventional Weapons. You know, each country looks at this differently. But I believe that's one of the reasons why in our marshal, we really focused on the State Department because the State Department has to lead this, not the Department of Defense. The Department of Defense should be right next to the State Department, but together we can really, I think, tackle this problem and make a lot of progress.

GENERAL ALLEN: Thank you. And, Eric, your last word, please, sir.

MR. SCHMIDT: Yeah, John, I was going to suggest that this is a pretty good task for Brookings. You know, that building these multi-stakeholder agreements requires patience, diplomacy, some time, and some sort of idea sharing. I don't think it's going to happen without serious amount of works in private sector like groups like Brookings and by our State Department. If I were to do it, I would try to pick the 10 countries that are likely to move the ball forward in this phase, and see if you can build a workable consensus among them on some of these issues. And I think the value of having those meetings in terms of mutual education, such as your meetings that you had with NATO, would probably be well worth it even if they're not very conclusive. This stuff is so new. People think they understand it, but they don't really. After it gets explained to them, they get depressed because it's so complicated. It's

a new paradigm. It's a new era. It's a new epoch for how people will work with AI and learning systems. There's a lot of things that can happen that people don't fully understand when the system is learning. And especially if it can learn in such a way that it learns the wrong thing. So, it's a new problem, right? And one which is well worth your time, our time, and our nation's time.

MR. WORK: And, John, let me just say. I want to make a shameless plug for you and for Brookings. For all of those listening, we've already talked about John publishing his thoughts on how AI is going to affect warfare. He has a new book coming out called, *Turning Point*, which is policy making in the era of artificial intelligence. I think it's coming this month right, John?

GENERAL ALLEN: It is, Bob. And I owe you a great deal for that plug.

MR. WORK: He wrote this with his colleague Darrell West. And so, you know, in my view, Brookings would be an ideal kind of institution to try to work through the issues just like Eric said.

GENERAL ALLEN: Well, thank you. I want to thank you both for an incredible hour. I just wish we could go on and on and on because it's such a rich topic. I would command to everyone's reading if you have not had the chance, the second quarter report of the NSCAI. It's very important reading. It provides our Congress and the executive branch an enormous number of recommendations and options that I think are so well (inaudible) that this can in fact ensure American leadership in this critical area.

And as you both said, in the end while it would appear that often this is a competition of technology in the greater competition, the great power competition of the 21st century, in the end it really is about values and first principles. And American leadership, not just in what we do in the United States with the private sector, what we do with our precious allies overseas, and the private sector overseas, can ensure that our values, our collective values and our collective principles are in fact that they will reign supreme in the context of technological advancement for the betterment of humankind. And that's really what we want, AI for good.

So, thank you very much for joining us this afternoon. We're deeply honored to partner with the commission and we will work closely with you in the future to further the work of the commission, but also to further the leadership of the United States in this important area. Thank you so much. We're grateful. Good day.

MR. SCHMIDT: Thank you. Thank you all.

GENERAL ALLEN: And, please, everyone stay safe.

MR. WORK: Thank you, John. And thanks to everybody who listened in.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020