The Future of Warfare: Gaining a Tactical Edge Through Cloud and AI

- Dr. Alexander Kott, *Chief Scientist, Army Research Laboratory*
- Lindsey R. Sheppard, *Associate Fellow, International Security Program, Center for Strategic and International Studies (CSIS)*
- William Schneider, Jr., *Senior Fellow, Hudson Institute*
- Colonel Jeff Kojac, *Department of the Navy Lead, Joint Artificial Intelligence Center, U.S. Department of Defense*

Hudson Institute, Washington D.C. Headquarters
1201 Pennsylvania Avenue, N.W., Suite 400
Washington, DC 20004
May 30, 2019

TRANSCRIPT

Please note: This transcript is based off a recording and mistranslations may appear in text. A video of the event is available: https://www.hudson.org/events/1695-the-future-of-warfare-gaining-a-tactical-edge-through-cloud-and-ai52019

WILLIAM SCHNEIDER JR: Well, welcome everyone. And I appreciate the opportunity to meet with you and, in due course, have a bit of a discussion about a very interesting subject, about the use of modern data sciences at the tactical edge. And to support our discussion is first, Alexander Kott, who is the chief scientist for the Army Research Lab in Maryland, then Colonel Jeff Kojac from the Joint AI Center in the Department of Defense, and Lindsey Sheppard from CSIS. So I think we'll begin with Dr. Kott.

ALEXANDER KOTT: Thank you very much. Yes, indeed, I am the chief scientist of the Army Research Laboratory - not just in Maryland, but in many other places around the United States and the world. And I need to start with an obligatory disclaimer. Anything that I say is my own views. They are not necessarily representing the position of the United States Army or any part of the United States government. And they are not intended to refer to any procurement action - past, current or future. And any interpretation to the contrary would be incorrect. Now that I did - it's the most important part of my talk, so let me talk about something that I think is very important. I'm not sure if we really appreciate the enormity of the technological upheaval - forget revolution - upheaval that we are living through. It is an upheaval of enormous scale, colossal. It's civilizational in nature, civilization-changing, comparable to the invention of agriculture or domestication of the horse. By the way, these changes tend to have tremendous impact on how we fight our wars, how we humans fight our wars - and - or invention and proliferation of gunpowder, things that change everything, things that really change the balance of civilizations, the way we live.

And I'm of course talking about the emergence of the artificially intelligent beings. And I want to emphasize, not artificial intelligence programs or artificial intelligence things, I'm talking about artificially intelligent beings because what's happening is an invasion. It's an invasion of a different artificial intelligent species - self-made, self-invited invasion into our human world. In a few years, we will definitely find ourselves - probably already finding ourselves - in an environment where we are no longer the only intelligent species on this earth. That's how momentous it is. That's how colossal it is. And, of course, invasions of new species or even new ethnic groups into the preexisting civilizations have never gone smoothly. And I wonder how smoothly this invasion will go. So this new artificially intelligent beings are numerous. Every one of you has an early form of that being called smartphone. Some of you have two of them. Some of them have three of them, right? And they probably already outnumber the number of humans on this earth. They're ubiquitous. They're everywhere. They're influencing everything. And they will influence even more and more in everyday life and in warfare. These artificial intelligent beings are voracious producers of information. And they are voracious consumers of information at the scale which was unthinkable just a few decades ago, scale that was simply unimaginable just a few decades ago. They are voracious communicators. They push that information everywhere. And of course, we are kind of unwilling co-conspirators with them in that process of massively multiplying communications throughout our world. They are much faster thinkers than humans. They can solve many problems much faster and much better and more accurately than humans. In fact, they solve many problems that humans simply cannot solve. They think in a very different way from what we do. They have different values. They have different way of perceiving world and formulating their thoughts. And we're starting to recognize it.

Look at all these programs that are starting to explain the ability of AI. This is just an early - this is just an early indication of how serious this is, this serious lack of understanding between this

new species and old intelligence species, us. At the same time, they're frighteningly vulnerable. They are frighteningly vulnerable to cyberattacks, to electronic warfare. They're frighteningly vulnerable to a variety of deceptions. Some of you have heard about something called adversarial learning, which is, I think, is also just an early indicator of enormous deceptive warfare that will be waged against this new species of artificial intelligent beings. And they're also threatening to all other beings because they are - because they can be taken over by the adversary and be used as weapons against other beings, human or artificial intelligent beings. And as I speak so - as I say so, I would like to remind you that we have no monopoly on the technology of artificial intelligent beings and no monopoly on this invasion. As you know, most of the smartphones you own are not made in this country. Many of them are not designed in this country. And the share of science and technology publications of this country continues to drop and drop and drop as compared to the rest of the world. So who will own the allegiance of those devices is an open question.

So now that I scared you enough, let me talk about ramifications of this invasion. And I prefer to focus specifically on the impact of this civilizational change on the tactical ground warfare, which is what I primarily do for a living and primarily what I know - the impact on the tactical ground warfare, primarily at the edge. And primarily, let's talk about data and communications. After all, that's what the organizers of this event promised you, so let's do that, right? So there will be, and already are, emerging very important changes that are engendered by this invasion of artificial intelligent beings. The rise of edge versus sanctuary - the edge of the battlefield might become actually more secure and more capable of defending itself than a sanctuary - some kind of a base, some kind of a presumably secure command post. And this is partly because of the emergence of the intelligent - artificial intelligent munitions, which will be able to go very far. We'll be able to find the target, and we'll be able to defeat this target in many different ways, no matter how far away from the front line it is located. So edge becomes more important. And that of course is very important for communications and cloud. Why do I say this? So the edge is where cloud has to be located, at least for the warfare. The connections to the reach-back data storage and data processing will not be reliable, will not be assured, will be subject to intercepts and manipulations, will be subject to jamming and elimination by other means. And the edge will need the data and communications right then and there and the edge, not back in Kronos, assuming Kronos is secure. And even that cannot be assured given all we know about the cyberwarfare - right? - as well as long-range resurgent fires.

So I believe in the cloud that is a fog, a fog that resides on multiple edge devices. And that's probably the most secure cloud we can find, something that is highly, highly distributed on small devices, continuously shuffling back and forth the pieces of data, the droplets of the fog - right? - in a way that will be difficult for the enemy to catch and to interpret. That's what I call the fog, the cyber fog, the place where it is the easiest to hide the data. I like that cloud. Now, that does not preclude other clouds. Other clouds are also very important. And I should remind you that I have no intention to refer to any procurement action past, current or future. But the fog clouds at the edge will be important. And small and many will be more important than big and few. Small and many will be more important than big and few because small and many will be far more survivable and far more capable than vulnerable big and few. So that's also important. Silence may be more important than communications. We need to learn how to communicate by being silent or at least very quiet. So many small, low-power artificially intelligent devices will be able to deliver information far more securely than a long-haul, long-range loud communications, which will be inviting - as soon as they start transmitting, they will be inviting a barrage of 155

millimeters. Resilience versus security - security is hard, especially cybersecurity; malware always find its way in.

So the question is not so much how we can assure the security, but whether our artificially intelligent agents residing on the fog cloud elements will be able to restore resiliently what they're supposed to do and get back into action. Diversity will be extremely important more so than monoculture. We are used to monoculture. Everything is one model, and we want to keep standards; everything should be standard. That's an - monoculture is an invitation for disaster as it is in agriculture, for example, right? One disease wipes out everything. One malware will wipe every device - wipe out every device. So diversity of cultures and subspecies of those artificial intelligent beings will be extremely important. And yes, we will have to learn how to live with multiplicity of standards and multiplicity of non-standard devices. I think we are witnessing the end of the network as we know it. The network that has been provisioned and established and managed and so on, that network is disappearing. Instead, what we will see will be a society, a self-organizing society of artificially intelligent beings that will figure out how to talk to each other and with the human beings and so on, a society versus network - which reminds me that humans will be gradually becoming a minority in the overall force on the battlefield.

Humans are already kind of reducing and reducing their presence on the battlefield as compared to other material. If you go back centuries, there were very few things on the battlefield and many soldiers. Now there are still a number of soldiers but a lot more things. And that balance will continue to go in that direction. So it will be the warfare of intelligent, artificial intelligent munitions, against artificial intelligent munitions and artificially intelligent software agents against artificial intelligence software agents. And humans will play a very important role, but that role probably will change dramatically as compared to what we know now. And I think we also will see the end of a traditional command and control. How do you command and control this multispecies force that lives by its own - sometimes incomprehensible to us humans - laws and intents and so on? So they're in with some other form of intentionality - are different probably from command and control as we know it. And with that, I am, I think, one minute over my allotted time. Thank you very much for listening. And we will be able to discuss some of this with the panel here.

SCHNEIDER: All right. Thank you very much. And we'll first have a couple of comments from our colleagues. Lindsey?

LINDSEY R SHEPPARD: Sure. So I think Dr. Kott made some excellent points. And while we are here today to focus on the tactical edge - and I think we will do that through the remainder of our talk - I think it is also important to recognize that in order to do the tactical edge well, we also have to do the enterprise well. And doing one well does not preclude the other. We have to do it well while keeping the other in mind. And absolutely, we need technical success at the tactical edge. But there are also many ways that doing cloud architecture and doing analytics and artificial intelligence within the Department of Defense enterprise and within the services can actually support the streamlined operation of that tactical edge. Logistics and maintenance, resource management are great areas where we can improve the whole enterprise that supports that edge network. And so I look forward to exploring the common themes that are in both the enterprise and the tactical edge and maybe the things that are unique to either one as we proceed today.

JEFF KOJAC: Just to add to those comments, I would say that when on the tactical edge, when the shooting starts, it gets really complex - right? - really difficult. And I'm encouraged that your vision, Alex, of fewer people on the battlefield, less bloodshed there, hopefully that - nonetheless is that as long as a people are on the battlefield, it's going to be a lethal situation - right? - and a difficult, emotional one. I think just to take a little bit more on your comments there - and that is, is that obviously, we're all familiar with the Clausewitzian Trinity - right? - where it's political, it's military, and it's also the society's populace that are involved. And I think what you're going after there, Alex, is that you're - we're looking at a fourth actor, right? There's a fourth actor coming. And that's going to be apparent both in this city and then it's also going to be an impact on the tactical edge. And when we're on the tactical edge, one of the things that we have to take into consideration is how we work with that fourth actor in a way that is safe, secure, ethical, responsible, that comports with our society's values. I think that's crucial for us to get it right. And I would hope that - I would think that we would. We've gotten things right in the past.

What's interesting to me, though, is the degree to which advanced technology - or I should say technology that runs counter to our expectations and our assumptions can get in the minds of the soldiers on the battlefield, as well as the politicians and the public. I'll use two examples of that really quickly, and that is punji stakes in Vietnam, which I know that was a long time ago for some of us. And then some of us weren't even born, but whatever - punji sticks in Vietnam, and then IEDs in the previous excitement that's happened in the CENTCOM arena. Both IEDs and punji sticks really got in the mind of everybody, right? It impacted how we looked at things as a society and also as people on the battlefield. And when we're talking about the introduction of a fourth actor, that promises even more disruption, I would think. And I would think that it's at the same enterprise level, whether it's bots helping us process the budget or bots helping us process manpower issues or how we acquire things, procure things through test and evaluation. We use RPAs for those things. It can dramatically change. But at the tactical edge, I would say that that fourth actor is going to be dependent on something that is heavily germane to today's topic, which is cloud computing, right? Because you really - you need cloud computing in order to train the algorithms, and you need the cloud computing to inform the algorithms and to access what's happening on the battlefield, both before and after. So I think that when we're talking about this - you didn't call it a revolution; you called it a...

KOTT: An upheaval.

KOJAC: An upheaval. This upheaval that is coming our way is that a foundation for that upheaval is obviously a cloud at the tactical edge.

SCHNEIDER: Thank you for the interesting remarks. I think the Colonel Kojac's observations about punji stakes and IEDs is - reminds us of how quickly the context in which these developments are taking place. I serve on the Defense Science Board. And nearly 50 years ago, the Defense Science Board did a study that became known as Assault Breaker I, or just Assault Breaker. It became a DARPA program which led to the instrument that produced the demise of Soviet military power in Europe by developing speed, stealth and precision. Accuracy was independent of range. Stealth was sharply diminished. Fifty years of Soviet investment in air defense and decision tools that were created to take advantage of surveillance precision strike and enabled the speed of decision to be inside the adversary's decision cycle, which was very important, and it just completely negated the core of Soviet military power in Europe, which was the ability to stage echelons of military power that would drive through NATO defenses.

What's - this suite of developments that we've been discussing that are basically exploiting the tsunami of data that's coming out of a sensor-rich environment is creating the basis on which we can evolve from the instruments that have produced success during the latter part of the Cold War to some opportunities now to - by operating at the tactical edge and leveraging data sciences and cloud architectures, to be able to mitigate further threats. And this is without failing to notice the risks that are associated with this capability as well.

The Science Board recently did - completed a study on Assault Breaker II, which involved the ability to integrate the data sciences and related technologies to it. So I think there are some really profound things that we can take advantage of - the cloud architectures, for example, when integrated with 5G telecom. 5G telecom has a very interesting and disruptive property because of the micro and picocell architecture involved, that you can integrate communications into the cloud-based architecture. So it's a very disruptive suite of technologies that are coming on faster than a lot of our institutions can absorb. So I think we have a very rich basis for discussion, based on the points our speakers have teed up. And I think it's timely to throw the - open to the floor for folks who have questions. Please give your name and institutional affiliation. Yeah.

AUDIENCE MEMBER: Culture is so critical here. And I was at an event - Genius Machines - a while back. And the head of DARPA basically said, you know, in the 1990s, the U.S. led the world in groupware technology. And I was part of that - I'm an entrepreneur. And he said in this big group of people, the key word in human and machine team is team. So my question to y'all is, what culture will baselines - do you see - and behaviors. We do project-based learning. We did first robotics. And we had - we have team-based stuff all over the world with robots. So what are the - do you see culture? What do we need to do to evolve culture? Because, you know, we have issues with other countries not because, you know - it's because of their culture and how they approach data, how they approach control, how they approach things. So how do you see evolving a team-based approach on the tactical edge?

SHEPPARD: I think culture is a huge part of this. So I appreciate that you opened up the floor with that piece. The reality is that companies, organizations and entities will fail to implement analytics and artificial intelligence if they do not change the entirety of the culture. When we bring in analytics or artificial intelligence into an organization, it requires a top-to-bottom recognition that analytics have to drive the organization, that I will perhaps be valuing different skill sets than I previously valued before - for example, more data scientists, machine learning scientists. And so I think there is a recognition within the United States. We are seeing it through various organizations that are saying, we need an AI strategy. We have the executive order on AI. We have - the Department of Defense has put out their AI strategy. But there is still a dichotomy of messaging that is quite concerning for me. So, for example, at the special operations industry event last week, the Special Operations Command chief data officer said that we need to demonstrate that there is a financial benefit to doing computer language programming and to doing these data-driven techniques. Great. I'm on board with that. He then ended that with, and we need to let the nerds get promoted. So to me, that says you may be, on its face, recognizing that something needs to change, SOCOM obviously being very much far forward on the tactical edge. But when you finalize that statement with, let the nerds get promoted, that tells me that the entire organization is not on board with valuing the skill sets that they bring to that organization. And until we recognize that, you can put a cloud computing architecture. You can put the best fancy sensors. But you have not addressed the culture.

SCHNEIDER: Yes, sir.

AUDIENCE MEMBER: I used to lead an NSF Engineering Research Center looking at some of these issues. And we've pivoted - at the suggestion, actually, of USC's president - to put together a multidisciplinary task force recognizing that, yes, there are armies on the ground - yes, there are ships in - naval ships in the ocean. But adversaries are attacking infrastructure inside the United States, attacking democratic institutions and processes worldwide. How does that get knitted back into tactics and tactical issues?

KOJAC: It's a fantastic question because, usually, a nature of this conversation emphasizes the military instrument of national power, right? And I think that what we've - we're already seeing that we're aware of is that we're in the middle of national competitions that are political and economic in nature. And obviously, there's plenty of - to use an old term - gray-zone competition and conflict going on. But the fact remains is that there's a huge emphasis by our competitors on the political side, as in domestic politics, and economic, as in economic competition between states. So when we're talking about this arena, the tactical edge vis-a-vis the military instrument, we lose that larger framework, right? We lose the big picture. And we focus narrowly on something small. I think that they're interrelated - right? - because they're interrelated - the defense industrial base is tied into the rest of the nation's industrial base. For us to get anything right, we have to do - we have to really do it between a public-private partnership, right? We're talking, ultimately, about dual-use technology.

Now, that might be a little bit spooky language for certain people that live in other states than Virginia or Maryland. But what we're really talking about is dual-use technology. And obviously, cloud is one of those dual-use technologies. It's to the advantage of the Defense Department, quite frankly, in acquiring advanced technology that is dual-use, that is commercial-based - right? - because we can acquire it faster. We don't have to go through all the prohibitive cost compliance issues, all the legal parameters that are required. When you build a tank, you have to buy it with certain acquisition rules that are completely different than when you buy a iPhone, not that the military would ever buy an iPhone, but it's completely different. So there's an advantage there when it comes to harnessing the cloud for tactical purposes, is that if we can use acquisition methodologies that are organic to public-private partnership, I think that that's beneficial to us. If we could just go backwards just for a second on the culture thing, and that is is that a lot of times when we talk about dramatic change inside of a defense establishment - and we are talking about tactical cloud being a dramatic change inside of the defense establishment - is that what drives change usually - usually - is a combination of political top-down pressure, right? Some elected official, whether they're in the legislative branch or the executive branch, some political appointee, somebody like that is driving the train. And that's in combination with a maverick inside of uniform. And that maverick inside of uniform, whether he or she, at whatever level, they are a participant in that dramatic change. And then the third vehicle for dramatic change that combines with the first two is intra-service - inter-service competition. If you noticed, I didn't mention anything about, like, foreign adversaries, right? So it's like political, it's maverick, and then it's - and it's interservice competition. And I think that - if you look at the landscape right now is that we have all three. So culturally, we can pull this off.

SCHNEIDER: Yes, sir.

AUDIENCE MEMBER: This question is to the panel as a whole. Given the profound quantum changes in AI that were described here today, do you foresee a third-rate power with strong

technological capabilities actually dominating first-world power either militarily or economically? And if you, do can you foresee or perceive any prevention means?

KOTT: Bill, this is for you, Bill.

SCHNEIDER: It's a good question because one of the characteristics of this kind of technology is the barriers to entry are relatively low. We've seen a case now where the city of Baltimore is at - on its knees because of a small criminal enterprise that's able to penetrate their information networks and prevent them - not only prevent them from using it, but using it as an instrument of extortion. So I think this kind of problem can be magnified. We've seen North Korea be able to operate on a scale that many larger countries are not - either not prepared or not able to do. So yes, small entities can become a very powerful force, which is why we need the kind of changes that have been addressed by several of the participants so that we're able to better deal with this. The discussion about the national infrastructure, for example, is very pertinent because as the commander of the Northern Command, which has responsibility for the U.S. territory, remarked that the homeland is not a sanctuary. China has a doctrine called "Unrestricted Warfare." It's unclassified, available on the NDU website that describes how they intend to attack every fiber of national power, which includes the civil infrastructure. And we have seen by Russia's evolution and its national security doctrine - the so-called strategic deterrence - goes right down to holding adversary infrastructure - civil infrastructure at risk. So yes, I think we have a full spectrum of nation states that are able to bring this kind of power to bear and to some extent perhaps even subnational entities and criminal entities.

KOTT: I think historically, major revolutionary changes in technology gave an opening for a smaller nation to play a much greater role than ever was imagined. Think about Vikings, relatively small and impoverished. That's a group. Think about Mongols. Major changes in transportation and mobility technologies gave them unique advantages, and they used it to their advantage.

SCHNEIDER: Yes, sir.

AUDIENCE MEMBER: Dr. Kott, it's good to see you. I'm happy you're here. As a chief intelligence person, just in general, is there anything that you can tell us that's, like, really, really cool that you've experienced, that you've seen, that happened, that you don't really talk about a lot that you could share with us, that's something that, even as smart as you are, you still are unable to explain or just something like that? Just give us all a treat that's, like, on a lighter note, that's not so serious.

KOJAC: (Laughter).

SHEPPARD: Thank you for letting Jeff and I off the hook.

(LAUGHTER)

KOTT: Bill, am I allowed to answer a question like this?

SCHNEIDER: No, it's...

KOTT: I am allowed. OK.

SCHNEIDER: No, you're not (inaudible).

KOTT: So let me suggest something. So what I did - I anticipated this question. And last December, I put together a video about 10 coolest scientific advances at the Army Research Laboratory. I was involved in some ways with most of them. Google them. Google them. They're really cool. They talk about all kind of things - new, unusual explosives - very cool - quantum communications and teleportation, about new kind of robots, about new kind of energy sources. It's all very cool. And just Google it, and you will have much better answer than I can give you within the next couple of minutes.

SCHNEIDER: Dr. Kott...

KOTT: Thank you for this question. And, yes, everybody, please go and Google. I put a lot of effort into that video.

(LAUGHTER)

SCHNEIDER: It had referred to some work that's being done at Dartmouth to try and develop an explainable way of understanding the outcome of the application of artificial intelligence to some specific problems because a lot of the outcomes are not intuitive. They are - they're going to be surprising, and that's driving this aspiration. So I think you'll see a lot of cool things out of that. Yes, sir, in the back.

AUDIENCE MEMBER: Yeah, I want to congratulate you. I think you're pulling, with your research, America's military into the art of fighting at the speed of light. I think that's what we're really talking about, which beats a lot of the hypersonics. We tend to move our information faster, so I think you're really on to something. Taking your title, "Gaining A Tactical Edge," each of your vectors is its own R&D program to the future, as are platforms - software, upgradable platforms going in the future the same way. So to gain a tactical edge, I'll go back to Nimitz at World War II, which he said, to gain a tactical edge, you have to train, train, train - the height of the war, that's what he said. So consequently, looking at it from the big picture, maybe Dr. Schneider, where do you make the practical marriage of your research on the big training ranges to have the operators - as the colonel said, a lot of the innovation percolates up from the mavericks, the fighter pilots, the silent - the SAD guys. I've been at Fort Sill - very powerful. So where do you drop these concepts and these technology vectors into the fighting force so that we can evolve together, crosscutting services, crosscutting domains? You know, Ellis, Yuma, Fort Irwin, Northern Edge - I mean, how do you see this going forward in the future to get that tactical edge to train, train, train?

SCHNEIDER: I am sure others have some views on it as well, but I think what we've seen with the way advanced technology is effectively introduced into military forces is by focusing on outcomes rather than the process by which the technology is is created or applied. And a nice property of advanced technology, even though it's complex, it also has the potential to make things simple because of the ability to focus on outcomes. And the opportunities today with the workforce that the military are dealing with are fundamentally different than, say, the conscription focus force that we had in Vietnam, where they were relatively short-term soldiers so that you couldn't have too complex a syllabus and expect to train the whole force. Now you have longer-serving soldiers. The educational requirements are higher than they ever were of, say, 50 years ago. But you also have digital natives that are coming into the force. And they are, in many cases, more adaptable to this technology than many of their officers. So I'm pretty optimistic about the ability of the forces to deal with it. But, Colonel, you may have an observation on this.

KOJAC: I do, Bill. So yeah, it's train, train, train. That's what I tell my lacrosse team of 12-year-olds. So I'm with you 100%. Train like you fight. So wear your mouth guards ahead of time. So I would say three things on train, train, train. The first thing is, is that I think what you're going after and was gone after previously is the absolutely - to, you know, act like we're Immanuel Kant is the categorical imperative of an AI-literate force. So we train our soldiers, airmen, sailors, Marines, civilians - we train them with regards to cyberdefense, right? Everybody has to go through cyberdefense. Everybody has to go through equal opportunity training. All that good stuff is that we need to also do some AI training. So we need this as an engine for creating an AI-ready force, an AI-literate force that's required for that teamwork that we've been talking about. So that's No. 1. No. 2 is that, fundamentally - is that when we're talking about algorithms, we're talking about training algorithms, right? And so to train an algorithm, you got to have just teraflops - hundreds of teraflops of data to train an algorithm. Now, then when you deploy an algorithm to the tactical edge, if you expect that algorithm to adapt to the fight, you still have to have massive amounts of data, and the only way you're going to have that sort of data at the tactical edge is if you have cloud, right? I mean, you just can't - you can't get there from here otherwise. So it goes to the imperative of cloud at the tactical edge - is the algorithms being able to train, retrain and fight again. And then the third part of that train, train, train is - you know, ultimately, when we're - training is not training for - you don't just train. In effect, every training exercise is a test. It's a validation. It's - the best things that come out of training are corrections. You did that wrong. Don't do that again. And so the same thing with algorithms, right? So right now, a portion of our enterprise writ large when it comes to algorithms is test and evaluation, which I would posit is part of training. And that aspect of test and evaluation - we are - I'll just - I think I can say this without being court martialed - is that we're dependent on FFRDCs and UARCs and things like that. And that ability to test and eval is something that we have to build - we have to be good at in order for us to train effectively. So your point is really strong.

SHEPPARD: We are making progress. Just to provide a few examples - because Jeff's third point actually highlights how important the first point is. I don't think any AI event could go without emphasizing how important it is to educate and train the workforce that we have as well as the workforce that we need because we can't neglect the folks that are in the door right now. So the Air Force has their Computer Language Initiative program where we are going to treat computer language programming skills as foreign languages, which laid the foundation for the armed forces' Digital Advantage Act, which expands that model to the broader services - only for military. I would love to see something similar for DOD civilians or, more broadly, civilians. But it's looking at - before I can throw our men and women into an event like Northern Edge and say, I want to put them in a simulated information warfare environment, they better know how to program, and so that's a good place to start.

AUDIENCE MEMBER: I will be the devil's advocate for a moment here because, basically, AI is great, but all of these things we're doing is adding and subtracting really fast. They can't even multiply, just add the same number over and over again. So - and what we have with, you know, machine learning is incredibly convoluted calculations which we may not understand, as users often - that match, you know, input to output, and we can get - that can make errors in ways no human could. EverServ (ph) AI, you mentioned - but their case is self-inflicted. We have, you know, racist image recognition that doesn't believe people with dark skin are human. It classifies them as apes. We have a program - one program that's been - Ted talked about was, you know, categorizing breeds of dogs, and it kept on calling huskies wolves. And finally, they realized it was because the background had snow in it, and all the previous pictures that had snow in it

happened to be of wolves. So, I mean, these things are also being - generally, AI may be coming - these things are very brittle. They're very subject to deception or bias in the creation unintentionally. So how do you guard against that? How you bring in the human as a corrective element without slowing everything down? How do you get the best of both worlds rather than the worst where the human is, you know, spaced out, inattentive, driving their autopilot until it runs into the, you know, white panel truck?

KOJAC: So obviously, what you're going after is what, quite frankly, is a nice summary of what was discussed before, right? So we have to go after the very real fact that, whether this technology is embryonic or whether it's fully developed in a few decades - is that it has to be handled safely, securely, ethically, responsibly, right? So it has to be - all the human imperfections that can reside in biases or imperfect ingestion of data because it was human beings that were part of that ingestion of data is - that has to be mitigated and has to be mitigated with an ethical mindset that reflects our society's values. Absolutely. Well - but also goes to what was said before with regards to training, right? So it's not that we're - the algorithms don't operate, or aren't supposed to operate in the future, in some solipsistic way. They're supposed to operate and function with human beings. So even if we're talking about, quote, unquote, "autonomy," we're still talking about human commanders, human maintainers. So there's - I think that it goes to the previous discussion of the importance that we have an AI-literate force, we have AI-literate political leaders, we have an AI-literate defense industrial base. If human beings are not part of the solution, we're buffoons.

SCHNEIDER: There's another couple of dimensions of this that are worth taking into account. While it's historically been the case that the DOD led the way for the rest of the society and the application of, say, computation - and that sort of, over time, trickled down into the rest of civil society. But the nature of AI is that the DOD activities in it is a small fraction of the global effort. And so there's a much greater generation of science and insights into this that probably is going to lead to more rapid improvement in the underlying technology. The second thing is in thinking about how technologies advance. When you have to go through the cycle of theory and experimentation, then recalculation, there tends to be a protracted period of time to improve a particular, say, line of an invention.

AI has the property shared by a few other technologies that have similar spooky risks, like genomics for example, where the underlying technology can be reduced to information. That information then can be reduced to software. That permits a much more rapid process of theory, experimentation, modeling and simulation and feedback in a way that advances the science much more rapidly. It's not to say that it'll be free of the kind of gross errors that you've described which underscore the risks of the technologies. But I think it's prudent also to expect that the technology will move much faster. Whether or not DOD is smart and absorbing it and adapting its processes and the other things remains to be seen. But it's a - this is - the thing that makes this technology so spooky in the way Dr. Kott has described it is because it has this property of a very rapid, perhaps even, in some cases, exponential growth.

AUDIENCE MEMBER:...With AI dealing with the physical world where there are physical life-and-death consequences. And that's just in traffic. You know, the battlefield is a much more dangerous, chaotic place. So that's - that raises a question for whether all the civilian exploration you talk about is always applicable, as well.

SCHNEIDER: Right. It's no doubt there's going to be many fits, starts, pitfalls and disasters. But there'll also be substantial progress. And I think if one drills down into where AI is being used successfully, I think it does suggest that there's some basis for optimism. Ma'am?

AUDIENCE MEMBER: Thank you all for being here. Your perspectives are really valuable. Appreciate it. Switching back to 5G for just a moment, what kind of - and this is for anyone - what kind of security infrastructure do you think that the U.S. needs to be implementing as of now in order to prepare for a 5G universe?

SCHNEIDER: The threats that are a consequence of 5G are much more substantial because of the capabilities that the user can invest into the technology. We see that China's concept of 5G integrates precision navigation and targeting through the - its coupling to its Baidu system. It integrates its surveillance technologies, as a Human Rights Watch report showed - that they have diddled one of their social media applications that they build into the Huawei phone, in this case, that allows the operator of the network to extract images from the user of the cell phone. And they're also - they integrate financial services into it through their cashless system. They're going to bring in a whole range of other financial services. So the consequence of having such a large inventory of data-based services from there requires a much different approach to managing the security function. With financial services, you would depend on financial institutions to do that. And in general, the kind of gruesome surveillance that we've seen in Tibet and western China suggests that that's not the kind of problem we have with AT&T and Verizon. So there's a whole new range of applications that need to be thought about if we're going to be able to have a secure environment with modern technology, right? I think there's probably not a technological fix to it. It has to be a policy-driven shift.

AUDIENCE MEMBER: Because I need a basic image that I ask this question - if there was enough AI technology during the Cuba crisis in 1962, how do you plan scenario (unintelligible) is my question.

SCHNEIDER: Anybody remember Cuban crisis?

KOJAC: I do. I do. I read the book, right?

KOTT: Then you have that - you are...

KOJAC: I mean, I can't be the only one, right? It's not just me and Graham Allison, right? So that's an interesting question. I would say that - so what you're positing is that instead of the president and his brother, the attorney general, saving the day by overruling the imprudent thinking of the Joint Chiefs of Staff and also our dear beloved Air Force general in Nebraska - yeah, LeMay - is that - what would happen if the president was relying on some sort of machine learning, some sort of deep neural network to analyze the situation?

KOTT: Yeah. That's exactly the question.

AUDIENCE MEMBER: I think - are you implying that we would have reached a decision faster? When I hear this question posited, it is often framed that the availability of information from machine learning and having the overhead assets and being able to do that processing would actually result in a decision to either escalate to use of force because they had information sooner. And obviously, we can't know that because that's in the past, but I will say that the assumption that more information always results in a sooner decision is not necessarily true and does not hold. Oftentimes - and this will be a significant challenge as we introduce more

machine learning capability into particularly our intelligence process and our analysis process - is that oftentimes, when analysts and decision-makers are faced with an availability of a large amount of information, you actually reach a decision inertia point where you start looking for that one piece of information that will take you from a 60% confidence to an 80% to perhaps a 90%. And so you spend time looking for that one piece of perfect information that will tell you, this is absolutely the decision I need to make, and that results in a protracted time between decisions being made, and sometimes, decisions not being made. So I appreciate the situation and the concerns that that scenario brings up, but there is a decent body of cognitive science and cognitive psychology that indicates that it doesn't always necessarily result in the decision being made faster. And that - both of those considerations have to be built into our systems and our analytic processes as we move forward and as we are flooded with the availability of more and more information.

KOJAC: So can I just take that to the tactical edge, like, really fast? And that is - so on the tactical edge, what you're talking about is that a platoon commander - a 23-year-old college graduate lieutenant being in charge of 30 people - is in a high-intensity, violent, deadly scenario where his own people have been killed and they've killed other people and a - some sort of small, micro-unmanned aerial system is able to look around the corner, so to speak, inside the village or inside the urban terrain or inside the jungle and determine - hey, these people that are around the corner are noncombatants. And due to the cloud computing, due to the machine learning that's involved, the predictive analytics, the computer vision - those algorithms all able to operate via a tactical cloud is that, as a result, that young 23-year-old platoon commander, instead of calling in fire on what's around the corner, is able to understand those are noncombatants and we're not going to kill them.

SCHNEIDER: I'd like to expand a little bit on the question about the Cuban missile crisis because if you look to a circumstance where, instead of just focusing on U2 overflights and monitoring maritime traffic going in there, with AI, there was a lot of other things happening elsewhere in the world. We had preparations for a series of nuclear tests which took place that week, the famous Starfish series of atmospheric tests in Johnston Island. Because the Russians tried to - the Soviets tried to put this force together to move the medium- and intermediate-range missiles, there was a lot of rail traffic, which was accessible but not monitored because of these kind of things in those days, and to a considerable degree today, are largely dealt with the intelligence community using classified sensors. But if you had AI that was scooping up all of this information - maybe my view is not shared by others, but having worked in the Department of State, if you know some of these things are happening earlier, you have opportunities to head off the crisis before waiting till it matures and the threat is upon you. And so I think that one of the great opportunities that we have with the application of artificial intelligence is to be able to fully integrate open source information with classified information so that you have much earlier precursors of how an event is going to spin out.

AUDIENCE MEMBER: Sir, I want to put a spotlight on an issue you raised earlier. One of my sins in life was I was one of the founders of the modern VA. And I learned a lot about medical computing. And in doing that, I watched the head of DARPA announce a brilliant $2 billion money throw at AI recently - made a lot of headlines. I'd like to remind the Defense Department that the American medical establishment has thrown an order of magnitude money it AI problems going further back in time than the Defense Department. All you have to do is go to a conference - an AI conference in American or global AI, and you will see dazzling - because

math is math, algorithms are algorithms, computers are computers - and they have the same security requirements with HIPAA - so consequently, they are a pacing function that really has done an awful lot of great work in AI. And that's a symbol of optimism to me in cross-cutting Cabinet departments like State to Defense, back over to the VA and others - just a point of elimination.

SCHNEIDER: Yes, sir?

AUDIENCE MEMBER: I kind of represent the - used to do the Golden Phoenix exercises. Are y'all aware of that? For several years from 2007, 2010, it was very live exercises where all these different groups got together. In chemical, biological, radiological crisis - you know, in any crisis, people have to get to Joint very quickly. And there are four words I have that certain clouds can do called coordination, cooperation, collaboration and handoff. Let's say you're future. We already have edge, joint edge clouds, joint data pods. Let's say that we've been working on it for years. What is going to be the IC barriers - because my friends tell me they're frustrated - in trying to do joint things? - because our culture, for many, many, many years, has been very stovepipe. Certain big organizations want to keep everything very stovepipe. So what is your view is - how do we move from this very stovepipe, top-down culture? What do you see as the catalyst to go to this joint - let's say we do all have these edge clouds and these edge pods, how do you see moving us to joint?

SCHNEIDER: One of the unfortunate things is that perhaps the adversaries that have the most heavy burden of centralization are the ones that are recognizing the problem. China created a strategic support force which integrates cyber, EW and space operations, strategic ISR, all into a single group so that they can share information. In the U.S. case at this point, we're emphasizing cylinders of excellence in the cyber command. We're setting up a Space Force. And there's likely to be other things that mimic those characteristics. How we create a joint enterprise out of these stovepipes that have a history of a very rigorous security to protect their own operations but not a history of sharing the information that have to be integrated in a multidomain context is going to be a big issue. But this is - it may be that AI will provide a catalyst for doing that because the value of these joint capabilities can be extracted by the use of AI. But that's an institutional barrier that has to be addressed.

KOTT: The problem of centralization and decentralization has been around for as long as human beings existed - right? - or, in fact, any biological species has existed. There is value in decentralization and specialization. And there is value in centralization and cooperation (ph). And where that dividing line is depends a lot on the environment and on the tools and techniques available to that system, right? If the tools and techniques favor centralization more than decentralization - so there will be a shift and an endless number of examples of that. So I agree with Bill that the increasing capability to integrate data in various forms, not necessarily by putting them into one big bucket, but by perhaps other means, and being able to make good use of that integrated data, which is non-trivial, and, you know, just putting more data together does not mean you will get anything better out of that. So the tools and techniques and methodologies will define where that dividing line is. I would not necessarily rail against the cylinders of excellence. They have their place. They have their value.

KOJAC: If I just add to that. So in talking vis-a-vis specifically the cloud is that, I think, that you're - what you're pointing to is that maybe we don't try to change human nature but that we try to make sure that our data is truly portable so that we can exchange the data between

whatever. Whether we're centralized, decentralized, whether we're human beings that are fallible or we're human beings that are perfect is that our machines via the cloud have a portability of data.

AUDIENCE MEMBER: I wanted to ask you a question - actually I guess is more specific bringing things back to the tactical edge itself and referring actually back to, Dr. Kott, what you said at the beginning about - or characterizing the edge cloud as being kind of a fog made up of particulates of data. And so I'd like to ask just the wider panel what you see as being the most appropriate tradeoff that - or tradeoffs - that DOD can make in terms of bringing these capabilities to the edge when eventually they are at the edge, when they are integrated into frontline operations. Obviously, frontline service members would like the cloud and AI capabilities they're using to be secure, to be resilient, to be redundant, to be interoperable, to be innovative and iterative. But there are going to have to be tradeoffs made in that decision. Dr. Kott, you seem to highlight that kind of a distribution and occlusion and the priorities in terms of establishing those capabilities. So I wanted to basically get just a sense from the rest of the panelists how you see these capabilities best deployed at the tactical edge.

SHEPPARD: So I would say there's - in thinking about it - and I appreciate your very systems engineering framing of the question in terms of tradeoffs and trade space and design space. The realities of the capability at a tactical edge is that they will be limited by virtue of the environment you are deploying into. And so I think there are three categories that we have to trade across. One is the data that we are collecting and that we are gathering. You are limited in terms of how much you can bring in. You are limited in how much you can communicate. Things like raw video feed and raw audio feed are quite massive in terms of when you're thinking about what bandwidth do I have available and what's the throughput? So as much as I can convert to digital, to get it into ones and zeros, or if I can be selective and strategic about what data I'm gathering and what data I care about, that's one way to address the capacity. Another way that is highlighted, actually, through our 5G conversations is if I can drive compute as far out to the network edge as possible, I'm offloading burden from not only the network bandwidth - or the network, you know, the bandwidth throughput of the network - but also the cloud servers. So one of the benefits of, you know, the 5G technologies that as we move things to the network edge, we're typically moving things off of the main servers and onto the device themselves by increasing the compute capability of the device.

A good example is we all have phones. Some phones - if you have an iPhone, you're not quite there yet. But you have the facial recognition to unlock your phone. Previous iterations required that image to be taken on your phone, transmitted over the network to a server. And the analytics were run on the image. And then it was sent back to your phone to say, hey, that is - this person unlocked the phone. As we have moved compute to devices, all of that processing is done on device, which means I now have server capacity freed up. So move your compute to the network. Be selective about the data that you're collecting and gathering. And finally, be strategic about your use of cloud architecture and cloud services because inherently if you want to have that capability in theater, you will have to have servers somewhere in theater. We have swap problems. You can only give them so much power. Think about putting a server farm in Afghanistan. So that means we have to be picky and choosy about are we bringing in multiple data streams? Are we gaining insights due to processing across those data streams? How do you use that server in theater? And then can I leverage the enterprise capability knowing that I may not have access to them to do the big heavy lifting that I don't want to do in theater? So I

would think about it that way. Think about the data, the compute, and then the devices that are actually executing that compute.

SCHNEIDER: I think another dimension of this about the need to force the - more of the capability to be available at the edge is that in dealing with the case of Russia and perhaps China, they already have a capacity to do submarine cable cutting, which means that a large fraction of the communications capability to reachback is going to be lost probably as the war starts because of the desire to prevent us from being able to operate at the edge, hence the need to think about making the edge robust, making sure they get the access to the right sensor data so that they can conduct operations efficiently at the tactical edge and to look to workarounds to mitigate the consequences of data loss from the reachback that's going to be an inevitable consequence of the disruption of tactical and strategic communication.

KOTT: And I really believe that ultimately we will see a fairly complex mix of reachback capabilities. We will see in theater tactical clouds that are of somewhat conventional centralized nature. And we will see highly decentralized cloud at the edge as well. And they all will help each other. And they will help - and they will all communicate to an extent. It is possible. And that's, by the way, is an interesting point about any enterprise solution for a cloud. One of the capabilities it should have is this ability to recognize that synchronization with the edge will not always be possible. And so it will have to be intermittent. It will have to be intelligent about when data will be or will not be available. We'll be able to kind of infer what has been missing. We've been disconnected for the last 45 minutes. Now we're trying to restore the state. OK, how do we do this intelligently? All these things will emerge, will have to emerge in order to make that possible.

KOJAC: Just on - since the attribute things were - attribute were addressed there is that one thing on process. And that is that if there was one thing to accept risk in and one thing to leverage more heavily, it would be on emphasizing agile rather than waterfall. So in doing any of these things, I think that the interface with the users is really, really important. So iterative interface with the - iterative - showing prototypes with the users not only to develop a better product but also to educate the users quite frankly and to generate buy-in - so it's both the product and also the human beings in doing the agile with the users as opposed to waterfall, you know, hey, we're going to design a tank and then 15 years later give you the tank. And the guys that designed the tank, they retired 20 years ago. So completely - I would go with agile as opposed to waterfall in the process of creating those attributes.

SCHNEIDER: A dimension of the agility is - also relates to training so that people are comfortable with being able to respond to this sort of disruption. It's only been a few years that exercise has allowed cyberattacks to play through to the end because it was often - or cyberattacks were not included in exercises because the game was over once cyber operations were introduced. And so now our forces are trained in a cyber-intense environment. And that is the kind of thing that we will need to adapt to to produce the kind of agility and resilience that we'll need to conduct tactical operations at the edge.

KOTT: And, you know, all warfare is based on deception. And I think it will be even more so partly because of AI and cloud. There are wonderful opportunity now to introduce extremely sophisticated deceptions through AI - by AI and for AI - and have it all nicely deposited somewhere in the cloud so that it can poison everybody's thinking (ph). Seriously, deception will be magnified. Opportunities for deception will be magnified as well as opportunities to find and

fight deception. So it will be an interesting world where some of the age-old stratagems will be transformed into a massive and much more sophisticated form of deception and counter-deception.

AUDIENCE MEMBER: Just a second question, on a more serious note this time - do you think that there are aspects of our lives and our reality that should be responsibly and professionally forbidden from artificial intelligence being able to be involved or accessed? Just for the folks who have lived lives and grown to be 70, 80 years old and you ask them, when they look back on their life - say, you know, what do you think could have been different and stuff like that? Well, I encountered a person that, you know, I really wish I knew not to ever deal with them, not to give them any of my time, any of my attention. I should have went a totally different direction, and my life would be totally different if I never even spoke to this person. Like, I really wish somebody could have told me that this is the person that would never do you like this or any - something like that. Like, could y'all speak to that aspect of where you don't think artificial intelligence should be involved at all? Thank you.

KOTT: You know, this is a very good question and a very difficult one to answer because on one hand, it is clear that technology can be inhumane, and maybe there are some areas of human existence where it should - certain types of technology just should not be allowed. And at the same time, there was endless number of attempts throughout the history of human - mankind to stop certain technologies from propagating through the society and being used, and they were generally unsuccessful unless there were some very good, very strong and very overpowering reasons to keep them away. And I don't know where this new wave of artificially intelligent beings will take us. It's a very good question, and I wish I had a good answer for it.

SHEPPARD: Well, I'm not 78 - surprise - but I do have one thought. And it's not necessarily where it shouldn't be used, but one area where I think we, as civilians in society, the various departments in the public sector - where we got it wrong was not understanding the value in data. And there were a few big players. We think of them as kind of the big tech giants who saw that value early and built up economies based on the value that data provides to your organizations, to your enterprises, to folks on the tactical edge. So ultimately, whether or not - you know, and bringing it back to the Department of Defense context, whether or not we get artificial intelligence right depends on if we can accurately elevate data to a strategic asset and, as an organization and as a culture, start to think differently about the value that data brings to our enterprises and our organizations. And a lot of the challenges that we see around - in the civilian sector, also - around questions of - is this an ethical use? Are we okay with this? - comes from that missed moment of recognizing the value that our data provides into artificial intelligence systems.

SCHNEIDER: We had experience in the laws of warfare that were developed in the latter part of the 19th century and early 20th century that were built around a shared recognition that there was a mutual interest in not using technologies of warfare at the limits of their application. So as a result - for example, in the pre-World War I context, it was agreed that you would not use types of bullets that would induce profound and lasting damage. And so it produced the jacketed ammunition and this sort of thing. It didn't eliminate the horrors of warfare by any means, but there was a notion that there was a shared interest in dealing with this at the limits of technology where it affected everyone. This realization has not engaged yet in the application of nonkinetic capabilities, and that's going to be a challenge to get people to recognize it because, as Dr. Kott suggested, the applications are so diverse and have the potential to change the outcome of a

conflict. That - it will challenge governments for decades to, I think, come up with some comparable laws of warfare kind of thing that affect data.

KOJAC: Bill, can I just add to that? And then I say, it's a phenomenal question, right? That's a question that a lot of people in the Pentagon - or plenty of people in the Pentagon are thinking about. So it's a really good question. We just take a twist on it and say that usually, when you lose a war, when you suffer catastrophe, it is because you didn't take into account what the other guy was going to do, right? So there's, you know, there's - the French in 1940 were not expecting the Germans to do what the Germans did. The - I mean, you know, there's plenty of books about that, right? So it's just as an example of the degree to which it's the unexpected, it's the unassumed that is going to get us, right? So we have to take into account that the bad guy, whoever the bad guy is, is going to do something to us that we - is not on our scope. We - the Department of Defense was not thinking that an airliner was going to crash into our building on 9/11 after two airliners went into the Twin Towers. That was not in any operation plan. So I would just say that what usually gets you is what you're not thinking about and what you don't expect. We are obviously - a lot of times, the human condition is that we can be our own worst enemy. But sometimes the other human being ends up being our own worst enemy. And you - and the way that enemy can exploit us is our failure of imagination.

SCHNEIDER: Yeah, go for it.

AUDIENCE MEMBER: Another question. Several people here have now mentioned, you know, the importance of getting large amounts of data to train the AI and how that is, of course, also a vulnerability. I have heard of lots of talk from, you know, DARPA and others about next-generation AI that has some kind of, you know, maybe perhaps in-built a priori knowledge or expert system component so it actually doesn't need to sort of trawl blindly through vast seas of data, that it can get by with maybe a trickle of data and still learn something. You know, what - where - what is the actual real potential for moving to that next-generation? How? You know, what are the approaches? How soon could we actually develop that? Or is it perhaps a pipe dream to get there?

KOJAC: So, Sydney, the real next step is synthetic, right? So it's the - so right now, the stage is, you know, a gazillion teraflops to teach the machine to do X, Y and Z. But the next step is - and it's already happening, right? It's already happening that we're using - we, the human race, not the Department of Defense - that we the human race are using synthetic data to train algorithms. So that's in the process. And that hasn't fully spelled itself out yet. As far as getting to a point where you're having an algorithm do really, really complex things in a complex environment through, for example, trial and error, that might - I mean, that can work on the chessboard or on the go board. But that's a lot more - that's a next-generation thing I would think. I don't know what next-generation means in years, but that's not today.

SCHNEIDER: One of the things that's being worked on in this domain is having more integrated modeling and simulation with experimentation, data collection and exploitation by artificial intelligence so that you do the modelling and sim and have that feed back into this loop so that you need less data on each iteration to be able to make some advances. And I think everyone in the field is trying to reduce the burden of data collection. And again, because this is driven by software, the prospect for rapid advance in reducing the data mountain that is needed to produce effective and reliable algorithms is likely to diminish.

KOTT: Sydney, my view is - not just view, but we actually at the Army Research Laboratory, we work very hard and have a number of efforts to get to, you know, learning from small number of data. There are a number of approaches. There's a, you know, incremental learning, when you use some learning, then you add a little bit data, and then you modify the underlying learned material. We are looking at learning by example when a human shows how it needs - should be done, and the machine, from a small number of examples - sometimes even one example - is able to learn reasonably well. We are exploring approaches such as learning with human critique, where the human provides occasional critique on performance of the machine, and the machine learns from that. So there are ways to do that. I am - you know, I am not going to prophesize when it will become practical. I - you know, I'm probably a descendant of prophets, but I'm not a prophet myself. And so - but there is certainly a promising - really promising - steps in that direction.

SCHNEIDER: Last question. Ed.

AUDIENCE MEMBER: (Unintelligible) Magic of computers. We tried Bayesian, decision matrix and decision theory and also Delphi. And we saw some promise in that. I don't know if that's going to drive AI or it's going to just be another subset of your skill sets in your tool box.

SCHNEIDER: Well, thank you very much. We've run out of our lease on this space for the day. So thank you for the participation and particularly the knowledgeable and insightful questions.

KOTT: Thank you.

SCHNEIDER: Thank you very much.

(APPLAUSE)