AI and Advanced Cyber Defense

This transcript is made possible through the sponsorship of Schneider Electric

Lt. Gen. Leah G. Lauderback:

All right. Good morning everyone. Good morning, Mr. Secretary. Thanks for being here this morning. Good morning. I am Lieutenant General Leah Lauderbach. I am a Deputy Chief of Staff for the Chief of Staff of the Air Force at the half staff at the Pentagon. I am otherwise known as the A-to-six. I've got the ISR portfolio, electromagnetic spectrum, and cyber in my portfolio. I'm joined today on a Valentine's Day, I couldn't be happier than to be with the crowd up here, but joined by Jade Baranski, who is the Chief Executive Officer and Co-Founder of Mobilize. Brian Morrison, who is the VP and GM of Space, Cyber & Intelligence Systems, General Dynamics Mission Systems.

Then, Tish Rourke, the Vice President of Cyber Intelligence and General Manager of Lockheed Martin. Thank you so much for being here today. We're talking about AI and cyber defense, and I want to preface this with the secretary, the announcements that the secretary and the chief made on Monday about AFCYBER and the elevation of AFCYBER. I'm going to ask the team here to give us some thoughts on if we're heading in the right direction, which I think that we are, and in elevating and understanding cyber, the domain, the personnel that have a responsibility for protecting that domain as we go forward. First though, I did ask the staff to start me off with some sort of a AI-generated poem, given that it is Valentine's Day.

You are going to be shocked at this as to what they came up with. What they looked at is they generated a haiku on love, AI, and cybersecurity. Here it goes. In circuits and code, love guards digital heartbeats, AI's safe embrace. Yikes. Yikes. Thank you team for providing that to us. But yeah, I think if you take out the love part, then yes, we've probably got some good way forward from an AI and a cyber defense perspective. We're going to dive right in and I'm going to ask the team here to start off each of the panelists, if they could introduce themselves. Then, just talk to us briefly for a few minutes on what it is that you're working on in AI and cyber defense. Tish, I'm going to start with you and then we'll go this direction.

Latisha Rourke:

Sure. I'll grab the microphone. Thank you, General, for having me here. I really appreciate that. I'm Tish Rourke, as she said. I run the Lockheed Martin Cyber and Intelligence organization where we're really focused on bringing together thinking of cyber as that fifth domain. We've got air, land, sea, ground. How does cyber become the foundation of all of those things? Because it's got to be the integral part. It's the first line of defense in warfare today. Ensuring that cyber is the first line of defense. Then, what we're really embracing now is how to embrace AI as part of cyber to get in front of, get ahead of the threat, not be reactionary to the threat.

Lt. Gen. Leah G. Lauderback:

Excellent. Thank you. Brian, how about you?

Brian Morrison:

Good morning. This is the only question I'll have from you, ma'am, that I'm the world's expert because it's just about what I'm doing. I'm privileged to lead the cyberspace and intelligence business at General Dynamics Mission Systems. The business is organized and focused almost exclusively on enabling our

customers in the department and the intelligence community to prepare for the cyber war that I believe we're in today and that I believe we'll be in tomorrow. That includes a strong focus on encryption. Crypto is really the core of much of cybersecurity. It also includes a focus on exploiting the vulnerabilities of our adversaries, which is something that gets many of us up in the morning. I'm deeply proud to be a part of that. Then, securing our own networks against our adversaries.

Lt. Gen. Leah G. Lauderback:

Excellent. Thank you, Brian. Jade, how about you?

Jade Baranski:

Yeah, thank you. Good morning, everybody. I'm Jade Baranski of Mobilize Vision and I am the CEO and co-founder. The first thing I'd say about the AI and data space is, we're really in that foundational, how do we build out structures to scale for the branches to work together? We've got a little bit different vibe than my counterparts here, but our product vision is the only joint platform that brings together innovation, process improvement, experimentation, RTDNE, all in one space for the DOD to work together. At our core, we're a data company. We hyper-focus on leveraging that data for faster solutions to the war fighter. As a founder of a startup, I believe that we need more of us in this conversation, and I'm proof that you can get there. We didn't work in the DOD and now it's been six years of being here with you all, and very privileged to be here. Thanks.

Lt. Gen. Leah G. Lauderback:

Awesome. Yeah, thanks, Jade. We're glad that you're part of the partnership for sure. Everyone on stage. Okay, so a first question that I have is, and it's really a foundational question, we throw out the term AI and we want to understand, or I would like to understand a little bit better. I know we've got some young Airmen and Guardians in the audience, that AI is a broad term that I think a lot of us use. I'd really like to get down to what your personal definition of artificial intelligence is. Then, how do you see that definition actually evolving into the future? Brian, can I start with you?

Brian Morrison:

I think we're at a particular point in the hype cycle right now, General, on AI. It's not a magic bullet, it's not a panacea. AI is probably not the discrete solution to any one problem. What I think it is though is a path to solution for many, many problems. Frankly, I think it's one of the most promising new technological paths we've seen, certainly in my career. When the layman talks about AI, I think generally people think of Chat GPT. The GPT here is generative pre-trained transformer, and that one in particular is trained by a large language model. Fundamentally though, I think we should think of AI as simply a set of logic techniques to separate signal from noise.

Because those logic techniques are automated, they can do it at a speed and a scale that the human mind is incapable of. That's really where I think the promise is. If you think about the amount of data we generate every day, we couldn't possibly assimilate all that data. We can deploy those logic techniques through AI to really filter, again, signal from noise. Sometimes those techniques operate in ways that we don't understand because the nature of an AI is that it's self-forming, it's self-reinforcing when it's done well. We don't need to understand what's under the hood of all of those logic techniques.

Of course, we need to understand the implications and the vulnerabilities of them. But it leads us, I think it can lead us to results that we could not have come up with on our own. That's my quick answer, General.

Lt. Gen. Leah G. Lauderback:

Yeah, thank you. How about you, Jade?

Jade Baranski:

Yeah, I 100% agree with everything Brian said, and I'll just add two additional things. First on Chat GPT, just a bit of perspective. It's really captured all of our imaginations. I think it's the greatest example, and not many technologies have made leaps the way that it has in our most recent, here we are, but I always like to remind myself and others that it's actually been in the works for decades. It's not new, it's new to us, but it's not new. Really thinking through what's possible today versus what's possible tomorrow gets really exciting. Just expanding on that, our definition of AI when we think about the data is really using the technology to give capabilities to humans beyond what we're capable of on our own.

Whether that's in some cases better efficiencies, which we love. Complex connections across domains, which Brian's pointing to, and you know what we're working on, faster decision points. All of it requires good data. The capabilities we believe of AI tomorrow require that we invest in good data today.

Lt. Gen. Leah G. Lauderback:

Yup. Great. Thank you very much. Tish, how about you?

Latisha Rourke:

Thanks. Of course, I agree with everything they said. I'll just probably add a couple things as well. The importance of AI in defining, making sure that we have what I call trustworthy AI. I'll just add some things that these guys maybe didn't talk about. Making sure we have trustworthy AI, making sure we understand where that operator in the loop is, because they're probably in a different place than they are today and where they're going to be tomorrow. Ensuring that we have trustworthy systems, assuring that we have resilient systems that can transform themselves for those vulnerabilities that we define, that we find, and make sure that we close those loops on those vulnerabilities very quickly so that the operator is free to do other things.

Hey, we've got the best operators in the world. They know their mission, they know what they've got to do. Let's use AI to help free them up to do more with less, as we always say. We have a limit. What we have now, the limitations we have today are things like swap and processing power. Well, every day Moore's law gets even better and better and better. Take advantage of Moore's law to continue to grow more, do more with less. Then, free up the operator to make those hard decisions and put them in a different part of the decision tree.

Lt. Gen. Leah G. Lauderback:

Excellent. Thank you, Tish. Okay. I'm going to ask Jade this question, but feel free to jump in if you'd like to, either of the other two. AI is a high-profile topic and it remains a frontier technology. With your visibility into the innovation ecosystem, what observations do you have about the role of AI in future conflict?

Jade Baranski:

Yeah, it's a great question. The first thing I'll say is I think we all heard on Monday, Secretary Kendall. Thank you for your remarks. You made it very clear to all of us that there has to be an efficient and effective pipeline of technology to the warfighter oriented around a very clear demand signal that aligns with where we send the investments, so that we can win the future fight. Did I get that right? Okay,

great. For a long time, "innovation" right has been a catch-all term, and we really mean getting after needed changes with novel approaches and emerging tech. We believe that data will drive that future. Today, we have all the branches with over 4,000 initiatives and over 6,000 joint users collaborating in that DoD innovation ecosystem.

That has been enough data to give us never-before-seen insights into that ecosystem in one platform, where leadership now has the ability to not only see those efforts, but know what's happening across the organizations. My favorite tactical example is you have a grassroots team, right? The warfighter sees a problem, probably doesn't think of themselves as innovators prior to this moment, but they say, "Hey, we got to solve this. The process of getting cargo onto an aircraft, this is no good. We're using carbon copy paper, yardsticks. This is pretty recent." They solve that problem in their own world for themselves, which is great.

Except no potential to scale that because they're in their little corner doing their job, doing the good work. But because that particular initiative was in vision, the innovation directorate at the major command level saw it and said, "Oh, this has major implications. We're talking agile combat employment, moving around islands quickly. We need to get this scaled." It has since been scaled to eight locations and it will continue to grow, but that's just one example of the thousands that we're seeing in the ecosystem that all have major implications. What we really want to do is that move faster. As you said, Tish, enable the people to move faster, make better decisions, and hopefully all with less work.

One of the strongest demand signals we've gotten from leadership, and this is very much the future frontier of AI in our system, is our newest feature. It's called Return on Mission Effectiveness. It allows innovators to tie their initiatives directly to organizational objectives. Think for the Air Force operational imperatives, the National Defense Strategy. What it does is it gives leadership a comprehensive view of how those lines of efforts tie directly to those strategies. Again, as was discussed on Monday, we believe that this future and where this is headed is the future of AI and it's beyond exciting. I just start to think about the ability recently at the Pentagon and talking about, we have all this data.

In the future, imagine this world where we could build out playbooks. For everybody in the room who needs to start something new, oh, you want to get into AI? Well, let's start with what's been done before, perhaps has it already been done? Oftentimes. What are the regulatory requirements before you jump into this AI? We know we're going to need it, but there's going to be rules. There's going to be regulations, ethics that we have to deal with. Giving that all to those folks in advance is something that this much data can provide us. The other thing I'd say is we all know, I think most of us know the innovation space is inherently disconnected.

We believe that the future roadmap is starting to engage federated learning to be able to access multiple environments so that we can cross-train our AI for better outputs with strategic needs. In this world, start to imagine a future where we can securely and without ever releasing any CUI data, be able to share successful acquisition strategies with our allies to rapidly meet our shared mission. I think Ukraine's success on the battlefield has been very publicly tied to their ability to move quickly and innovate. With this type of capability, we'll be able to incorporate relevant and releasable solutions and pathways to our allies and partners, which we've never been able to do before at any scale.

We think in this AI-powered future, Airmen and Guardians will be on the leading edge of the conflict. You're the ones who are going to encounter the capability gaps. You personally can then go identify the need, source the collaboration, and communicate the strategic value to leadership, and we're talking a timescale of hours, not years. I think to be clear for us, we don't believe there's any future conflict in great power competition where humans alone can meet the moment. It's just adding to. We believe that the stakes are incredibly high, which was basically the theme of the opening remarks. China's ability

to commit its massive resources to developing capabilities is that asymmetric challenge that we have to overcome.

In future conflict, every service member will be personally responsible for being able to adapt to the changing circumstances on the spot. We really do all have skin in this game of change today.

Lt. Gen. Leah G. Lauderback:

Thank you, Jade. I'm glad that your team is on our team and helping us with that conflict in the future. I want to pivot then to, let's talk about cyber defense. Thank you, Jade, for bringing up China and the threat that is posed to us. We know that our cyber attack surface, excuse me, is expanding at the same time that our adversaries are building out more advanced cyber capabilities. Brian, over to you. How can the DOD leverage AI to ensure quick detection of these types of threats and improve our cybersecurity posture?

Brian Morrison:

I think we could spend days, General. I guess I'll start with the pedestrian and move to the more ambitious. At the pedestrian level, we already know that somewhere north of 80% of all cyber attacks are rooted in known vulnerabilities and known attack vectors, but we still leave our doors and windows unlocked because our networks are massive and were humans and we're fallible. Just in a very pedestrian near-term way, I think deployment of well-tuned and trained AI agents can help us to increase our sort of what I would call compliance level on our networks. Of course, there are automated compliance tools today, but those compliance tools rely on the right inputs and they themselves rely on the right maintenance.

We can automate all of this with AI and reduce our attack surface in really meaningful ways in I think really short order. The second area, I think Secretary Kendall has been talking since he was under Secretary Kendall about the need for velocity of development and velocity of innovation. I think AI shows great promise there. If you talk to a software engineer and they're candid, they'll admit to you that a lot of software design is frankly Googling. We seek snippets of code that exist in the world and integrate them into whatever we're doing, and then make the necessary changes and check to make sure it's going to work and not break the system. Then, we roll it into production.

That has the flaw that we import flaws, and it also means that our imagination for the way we write our code is limited by what already exists in the world. This is not a limitation that a good AI will have. They can generate code faster, in maybe more novel and processor efficient ways or user efficient ways than we otherwise could. Now, that's not just limited to software, of course. When we use an AI to brainstorm innovation, we don't envision an aircraft wing that looks like every aircraft wing we've ever seen. We might envision an aircraft wing that looks like something more out of science fiction, that looks like an alien technology.

That's part of the promise of AI in the development world, that it will help us expand the boundaries of our imagination and leave behind us the cognitive hindsight biases we all have as human beings. Specifically in the cyber world, I think the third really promising area is in attack detection. When we have a cyber attack on our networks or our weapon systems, they generally rely on some alert system to tell us an attack is going on. Then, there's often a human in the loop to say, "Okay, what's going on? How do I explain and understand this anomaly, and how do I remediate it?" Then, there's a years-long process of cyber forensics to find out how that happened. Well, AI agents aren't bound by our speed of thought and information ingest.

You can have deep learning models that ingest massive amounts of information to really respond at network speed to those kinds of problems. That allows us to detect anomalous network flows, again, at

machine speed and at least immediately stop those flows and then assess what's going on. We're probably going to need a human somewhere in the loop for good legal and compliance reasons, and frankly safety, but they can allow us to drive velocity in that process also. I would say the fourth and maybe a little bit further out is, whenever I think about AI, I immediately think about the risks and vulnerabilities that we bring onto ourselves when we deploy an AI. Because if you can bias the training of an AI, you can really skew the output.

We always have to be cognizant that our adversaries are going to be trying to do that. Well, that means we should be doing the same. I think AI holds great promise in probing our adversary's networks, in exploiting their use of AI in ways that we haven't really even conceived of today.

Lt. Gen. Leah G. Lauderback:

Thank you. Tish, did you have any thoughts on that question as well?

Latisha Rourke:

Well, I'm going to pull it, maybe think about that question from the perspective of, how do you take what Brian said and apply it to what are we going to do about our workforce? What is the future of the workforce? If I've got AI, do I need all these STEM? We say, hey, there's a war on talent. But from my perspective, I think about, hey, 50 years ago we talked about the world was afraid, oh my god, I'm not going to have a job because a robot's going to replace me. I think this whole AI initiative, what we're doing enabling AI across all of everything that we do is actually driving the need for more STEM, along with this compliance piece. How do you bring compliance and ethics into STEM? It's I think a subtle part of it now, but even more so in the future.

How do you take that? How do you take that and say, okay, as Brian talked about and Jade talked about, how do we ensure those vulnerabilities? How do we think with the end in mind with AI? How do we tell our AI systems to... what is the outcome we want? Then, reverse engineer it as opposed to, hey, go do what you want and then we'll figure out what the vulnerabilities are. Let's go design in the resiliency. Let's go design in machine learning to self-heal. How do we get those STEM initiatives in academia? Hey, our research institutes are doing that. The defense industrial base is doing that. All three of our companies, small and large, are doing those types of things.

We're going to need more, not less. It's going to change where that, as I said earlier, it's going to change where the human is in that loop and how we ensure that we are effective on the battlefield. I often think about also just the evolution. I think we're in an evolution now. There's going to be a tipping point where that evolution's going to become a revolution, and we have to think differently about how to use AI, how to use machine learning, and where to put that operator in the loop.

Lt. Gen. Leah G. Lauderback:

Thank you, Tish. You already started to answer part of my next question, so I'm going to reframe it though, and for anyone. Of course, the announcements that we also made, not just about the AFCYBER, the elevation of AFCYBER and the importance of understanding cybersecurity and any other aspect of working in the cyber domain. But we also talked about warrant officers and we talked about technical tracks just a little bit. Hitting on what you had just mentioned, the balance of this workforce that we have, we know we've got to have the technical expertise, and I loved your comments there on probably needing more of those types of folks.

What would you think, if we talked about more technical tracks on the officer side and perhaps on the enlisted side, and then, certainly the warrant officer program that we're going to introduce here this year in cyber and IT, any thoughts to that?

Latisha Rourke:

Well just maybe a quick response here, but boy, whether it's your warrants, you're enlisted, whether it's your officers, and I said this in engineering school, we teach everybody how to solve hard problems, and that's what you do every day. Where do we leverage the machine learning to do that and where do we need those smart people who say, that's not how it's going to work on the battlefield. The battlefield just isn't being fought in one spot. The battlefield is a multi-domain operation, so being able to share that information instantaneously to get to those quick decisions is the importance of how we need to move forward.

Lt. Gen. Leah G. Lauderback:

Okay, thank you. Brian, any thoughts?

Brian Morrison:

Yeah, so I think we all recognize that one of the principal challenges of being in the military is that just when we get good at our job, we go do a different one. My own experience in combat with army warrant officers was that they really performed, I hope this is part of the rationale, sir. They really performed a distinct role by being that long-term domain expert. I think that it shows great promise for the Air Force and the Space Force to have those long-term domain experts, particularly in the cyber and IT fields. They performed, certainly in the Army and the Navy, they really performed a role in educating everyone else who's rotating to a new domain all the time about the importance, not the importance, sorry, the specific details and challenges that are unique to that domain.

If you're here in this room, you agree with me that there are challenges that are unique to the cyber domain. I think it's going to be a tremendous force multiplier for the Air Force, Ma'am.

Lt. Gen. Leah G. Lauderback:

Great, thank you. Any thoughts to that?

Jade Baranski:

Just the good news, that there's thousands of people that are already in that space ready and willing. We work with them every day.

Lt. Gen. Leah G. Lauderback:

Yeah, thank you. Yes, I think that it's such a great partnership that we do have with industry and your workforce, as we might be trying to pull some folks or we'll just use you through. Thank you. Thank you. All right, so this last question that I had here, it was talking about the, asking about the right balance between the specialized personnel and automation and AI capabilities. I don't know if we have any other thoughts to that or... Nope? Okay, good. Thank you. All right, and then I'm going to move on to a final question before we we'll close it up. Digital transformation and what the future looks like for digital transformation. Jade, can I ask you to start?

Jade Baranski:

Yeah. From our perspective, having gone through this, I'm going to call it a process, a journey, a long pathway, starting with hundreds of stakeholders with that outcome in mind. Tish, to your point, we all had the same outcome in mind and in the beginning it was, well, I love my SharePoint. I'm used to my

SharePoint. Don't take my SharePoint away from me. All the way over to the folks who were using Trello.

Brian Morrison:

Gee, I've never heard anyone say that about SharePoint.

Jade Baranski:

Listen, listen, you don't know Kathy Reed, she loves her SharePoint. There was that big range, including the teams who really, when you think about modernization, they had their whiteboard and they had sticky notes, actual sticky notes, tracking real data, some of which I would argue was pretty important. That mindset took years to bring together early value, starting to show some quick wins in the system, really listening to those stakeholders to say, "We're not going to tell you the answer. We're not going to tell you the right way to do this. We're going to work with you and we're going to iterate." One of my favorite just facts about Vision is that we've released over 4,000 significant releases.

We're not talking a word or a change, like groups of changes since we went live two and a half years ago, and that's a lot of work. It's a lot of engineering, but that ability to listen, work with industry, solve the problems one at a time, and not try and eat that whole elephant in one bite, because it wouldn't have worked. I can tell you now from perspective that had we gone after the end solution from day one, it would've been a massive failure.

Lt. Gen. Leah G. Lauderback:

Yeah, thanks. I think that hits on the integration aspect and our operational imperatives that the Secretary has driven us toward bringing industry and the operators together at the very beginning to understand and iterate through that whole process.

Jade Baranski:

Yeah, I tell every cyber phase two company, you need at least a hundred stakeholders. I am not joking, at least a hundred. They look at me like...

Lt. Gen. Leah G. Lauderback:

Yup, got it. Thank you. Yeah, digital transformation. Any thoughts on the left side here? Go ahead.

Brian Morrison:

I think that many of us in the room recognize that our, I'll take it from a higher level of granularity, many of us in the room recognize that our technological edge over our principal one to maybe three adversaries has eroded. We no longer have that huge offset that we had. We've got to do things differently. I think we all agree. To me, that's the promise of digital transformation because if we keep doing things the same way we've always done them, I'm lapsing into axiom. If we keep doing things the way we've always done them, we're going to get the same results. I think we need to really invest in digital transformation.

Certainly, the Air Force and the Space Force are doing that in spades. We've got to start getting at regaining our technological edge, preserving that technological edge. I don't know any way to do that than with deployment of tools like AI and really investing in digital transformation.

Lt. Gen. Leah G. Lauderback:

Thanks, Brian.

Latisha Rourke:

Just addition to that, I think of the thought, we're only as strong as our weakest link. If we don't embrace digital transformation, we don't embrace AI, we're only as strong as the weakest link. We're going to be very weak. We've got to embrace continuous integration, continuous development. We're used to deploying systems and then three years later providing an update. We've got to do things like provide cyber resiliency, cyber training, cyber readiness in a continuous integration, continuous development process that provides updates every two days. If there's something that's needed in the field, let's deliver it to the field, let's deliver it to the theater, let's deliver it to those multi-domain operations.

The only way we can do that is if we embrace digital transformation. That's not just for the military, that's for the whole defense industrial base, and our suppliers that are in defense and in the commercial world. It's got to happen.

Lt. Gen. Leah G. Lauderback:

Excellent. Thank you. All right, I know we've only got a few minutes left here, so I just wanted to open it up to each of you if there was anything else, a message that you wanted to get across, and then I'll finish it up. Jade, how about you?

Jade Baranski:

Sure. I'd love to start. Thanks. For those of you in the room who are Airmen and Guardians or any other, you're in any other branch, please come see us at booth 1609 and sign up, because there really is a way to get involved today. We've got a whole team here. We're relatively local-ish out of the Denver area, so we have a big presence. We'd love to talk, show you the system, see your use cases, and really share some of those outcome-driven wins that we've already seen. Come see us.

Lt. Gen. Leah G. Lauderback:

Thanks, Jade. I think, if I remember correctly, we do have a link with the SkillBridge program.

Jade Baranski:

Yeah, over a quarter of our team came directly from SkillBridge. Yeah, if you're into that kind of thing, you can come talk to Bo. He's right here in the front row. He has a SkillBridge-er. He has SkillBridged.

Lt. Gen. Leah G. Lauderback:

Awesome. Thank you very much. Brian, how about you?

Brian Morrison:

Secretary Kendall has talked about our technological edge as a deterrent to war, and particularly with our principal adversary. We are already at war in the cyber domain. I really want to encourage all of us to think about our use of AI and our adoption of AI as a way to really preserve and expand that technological edge. It's not about delivering a new tool, it's not about delivering a new product. It certainly isn't about selling something to the Air Force and the Space Force. It's about preserving peace in the world. That's what our technological edge gives us, and that's why I think the stakes for AI are so high, and that's why I'm proud to be a part of it as your partner.

Lt. Gen. Leah G. Lauderback:

Thank you very much. We're happy to have you. Tish?

Latisha Rourke:

My last plug is going to be, once again to plug and encourage STEM education to encourage us to... We still don't have enough of a workforce, so let's continue to encourage that STEM education. But in doing that and encouraging kids to go into STEM, you look at the workforce today and they think differently about going to work every day. Yes, we're in an environment where a lot of our work is classified, but I believe a lot of our work isn't. How do we create an environment, a digitally transformed environment for the workforce? Can they work from home? Can they work when they're in New York or when they're in California, or when they're in someplace else, and then only have to come in to do classified work? We're backlogged with clearances.

If we can open up some of those apertures, we can open up the number of students interested in STEM and wanting to come into this workforce. AI is something that's, they want to do stuff with AI, they want to be part of AI, they want to be part of the mission, but they want to do it on their terms. Not only do we need to digitally transform and think about AI for what we're doing in our mission, but in how to attract our workforce.

Lt. Gen. Leah G. Lauderback:

Thank you. I appreciate that very much. As I was thinking about the summary of the panel today, the informing or educating all of us from a workforce perspective on AI automation, augmentation, what it is that we can do in the cyber domain and beyond the cyber domain I think is extremely important. The informing though, for me, also is about understanding the threat. We didn't hit on it too much today, but that threat is real and that threat comes from a number of different adversaries out in the world for us. We have a personal responsibility, I think, as far as understanding that threat and then a personal responsibility to secure our personal data perhaps. Then, of course, our professional, the data that we are using to do our job with every single day.

Thank you for that. I also wanted to really just hit on the re-optimization that we are unveiling this AFA. The re-optimizing our entire workforce and many, many elements, of course, of the Air Force and the Space Force to get to a better place so that we can secure and we can do deterrence at first, but then if forced to into a conflict, we can win in that conflict. You all are a big part of that, of course, as our industry partners. I very much thank you for being out on the leading edge and then helping us in the journey that we are on today. Thank you very much. Thank you everyone in the audience for participating today and listening and learning a little bit.

Then, the last thing I'm going to say is that, don't forget Valentine's Day. Please hug your spouse or something. Okay. All right. Have a great rest of the AFA. Thank you.

This transcript is made possible through the sponsorship of Schneider Electric

Schneider Electric