

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

This transcript has been edited for clarity.

BOWMAN: Welcome and thank you for joining us here today – for today's event hosted by the Foundation for Defense of Democracies. I'm Bradley Bowman, senior director of FDD's Center on Military and Political Power. It's Thursday, October 1st, and we're pleased to have you here for this conversation, some in person, some tuning in live, some listening to our podcast.

The world is witnessing an AI race primarily between the United States and China, and that race will impact nearly every sector of our lives and our societies. That includes the U.S. military, of course. But the conversation around artificial intelligence and warfighting often centers primarily on development and the race to build the most capable combat systems. Those efforts are certainly vital, but they are not enough.

In this competition, the advantage will not simply go to the nation that builds the most powerful model first or the systems that can go through the detect, decide, deliver kill chain the quickest. The advantage will go to whatever government can also put the capability to work most effectively across the entire military enterprise. That's obviously easier said than done.

But in this race with China, the United States has some advantages. America leads it in AI development. Most of the world's top frontier labs are American. That gives the Pentagon a running start in the effort to translate AI innovation into tactical, operational, and strategic advantage.

And thankfully, the Pentagon has not been sitting on its hands. The Pentagon awarded contracts to a number of frontier labs. They've – leading to the rollout of GenAI.mil and the release of an AI Acceleration Strategy. These are important steps, but we should avoid over-confidence.

China is our principal competitor in this race, and Beijing, of course, is not operating by the same rules. Chinese firms have been stealing American AI intellectual property and using it to train their models, reducing the costs of development and helping the Chinese Communist Party run faster in the high stakes AI race. That will help make the People's Liberation Army more lethal and will impact the balance of power in the First Island Chain.

Worse still, prudence requires us to assume that China will increasingly share some of its progress in AI with Russia, Iran, and North Korea. The Chairman of the Joint Chiefs of Staff General Dan Caine testified before Congress in June 2025, as I've said, that Beijing, Moscow, Tehran, and Pyongyang are, quote, "pursuing unprecedented levels of cooperation that extends across military, cyber, economic, and informational domains," end quote, as we document in our new book on the Axis of Aggressors.

So, what's to be done, not just with flashy combat systems but across all facets and all levels of the Department of Defense, including in education, organization, and resourcing? What are some historical comparisons that might be useful? And what are some urgent steps we need to take now?

To discuss these questions and more, we are joined by an outstanding panel.

My friend and colleague RADM (Ret.) Mark Montgomery is the senior director of FDD's Center on Cyber and Technology Innovation, and directs CSC 2.0, which implements the recommendations of the Cyberspace Solarium, where he served as executive director. He previously led policy for the Senate Armed Service [sic, Services] Committee and spent 32 years in the U.S. Navy, retiring as a rear admiral in 2017.

Major Megan Hainline is an officer in the United States Air Force, the chief of Air Superiority Programs at the Secretary of the Air Force International Affairs Weapons Division, and a – and I'm proud to say a visiting military analyst here at FDD. She has more than 10 years of experience as an F-16 pilot, accumulating 290 combat hours.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

Isaac Harris, CDR USN (Ret.), is an adjunct senior fellow at FDD's Center on Cyber and Technology Innovation, and executive director of the Frontier Security Institute. He served 23 years as a U.S. Navy surface warfare officer and held positions such as policy advisor to the secretary of defense on China, technology security, and senior professional staff member of the House China Select Committee.

Leah Siskind is FDD's director of Impact and an artificial intelligence research fellow at CCTI. Prior to FDD, Leah served as the deputy director of the AI Corps at the U.S. Department of Homeland Security. She spent four years with the U.S. Digital Service in the White House, where she led efforts to modernize government technology. Her private sector experience includes roles in data and analytics – analytic companies such as Palantir and Uptake.

Before we dive in, a few words about FDD. For more than 20 years – well more than 20 years, FDD has operated as a fiercely independent, non-partisan research institute exclusively focused on national security and foreign policy. As a point of pride and principle, we do not accept foreign government funding. For more on our work, please visit our website, [FDD.org](https://fdd.org); follow us on X and Instagram; and subscribe to our YouTube channel.

Mark, the floor is yours.

MONTGOMERY: Hey, thank you very much, Brad. Thanks for your leadership in our military and political power team here. And I want to get started and get right into it.

I also think – I want to thank the U.S. Air Force for allowing Napalm – Megan to work with us on this. This a precursor to a significant paper coming out that the – Megan has written and I think will, you know – will provide a lot of detail to go along with the discussion we have today.

So Megan, when people hear military AI, they, you know, they think of Will Smith, you know, and a robot running around. But in reality, you know – and then the press coverage really pushes that, and it pushes it when you watch, you know, Ukraine. You know, the exciting ground robot is the one that, like, just looks like a ambulance pulling someone out. But the one they show you is the one where, like, a M60 machine gun on it, you know, killing Russian soldiers. So, we really amplify the kind of automation in AI.

But you argue in your paper, and I hope you'd argue here, that the real advantage for the military is less dramatic than that. Where do you think the real aggregated value of AI is going to come for the military? And how can we best use it going forward?

HAINLINE: Yes. Thanks, Monty, for the question, and thanks to FDD for being here today.

So, you're right. I think when you look up AI in the military, where people's minds immediately go is the drone swarms, the "I, Robot", the extreme end of automation and of physical form. But what – looking at AI as a general technology and looking at the broad use cases that AI brings to the table really unlocks a lot of other uses that remove friction from just daily operations for hundreds of thousands of warfighters.

And that is where I think the aggregate value of really implementing and ensuring AI per – is diffused across the force is going to be more powerful than having a few units that have drones or have some robotic system.

So AI in general is hard to pin down in a definition because there's so many use cases, everywhere from your chat bots with a large language model behind it, the, you know, imagery and video analysis or generation, your technology that enables self-driving cars or your drone swarms, to a bot that can play chess or Go. There's this broad swathe of use cases and applications, both in the physical and in just the information realm.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

And so, making sure that we're not just focused on the drone swarms and the high-end actual tech pieces and using it like an engineering solution to a problem, but thinking about using AI to reimagine our processes. Not just automating bad processes but completely revamping what we're doing at – just in a day-to-day operational context.

So, your maintainers that are right now on paper updating what they have done for the maintenance logs and having to go put that in Excel or some other program that gets updated. Not knowing if – when a part breaks on the airplane, is that going to be readily available? Do we have it on hand? All these things that just add friction to daily life; that they can be fixed if we were to apply this new technology smartly to existing processes or revamp those existing processes.

So, your logistics. Your mission planning is huge. We spend a lot of time manually creating things in PowerPoint or Excel and just coming up with ways to convey these complex things, these operations we're going to go do.

And if you had better systems behind that to remove the two hours, you're about to go waste moving arrows around on a PowerPoint just to convey this to senior leadership or to everybody else to get people on the same page, those are hours you get back. That all of your warfighters can spend on the actual job and the really high cognitive tests that you need people to be doing and that machines aren't as good at.

So, I think the current approach can tend to lead a lot of people throughout the military to feel like someone else is doing AI. It's not their job; it doesn't have direct impact to their daily life. But if we were to approach it more of a – it – there are all sorts of processes we should really take a hard look at and take ownership to use AI and advanced compute to reimagine, then a lot more people could be implementing it. And that's where you're going to see a huge aggregate value in just hours saved, where you're not wasting time on things that don't matter but you're spending time on the things that do matter. And that's where your military advantage is going to come from.

MONTGOMERY: Well, I'm glad you took it right down to, like, the most aggravating part of the military, you know, developing power – taking and developing PowerPoints.

(LAUGHTER)

(CROSSTALK)

HAINLINE: Yes, (inaudible) this morning. Yeah.

MONTGOMERY: I do – you do make me think, though, that –when I think about what is, like, killing the Navy, it's shipbuilding. And the idea that our shipbuilding is – you know, there's – I don't think there's enough machine learning in AI and U.S. shipbuilding processes. And if we could bring them in, we have got to be able to make that more efficient and effective than it is right now.

And that's – so this kind of – the non-weapon and non-war plans end of AI really has a lot of opportunity in the military. Hopefully in your paper, that'll really be drawn out so that we can – we could emphasize that, because that – investment in that could pay off even bigger than investment in the weapons system.

HAINLINE: Definitely.

MONTGOMERY: Well, Leah, you've been looking at the other end of AI, you know, as – for a – over half a decade inside government, thinking about AI misuse. You study adversarial actors and how they use AI against the United States.

Look, Washington's having a long debate right now on the kind of AI safety risks and, you know, doomsayers versus, you know, aspirational investors. And, you know, right now, what do you think is the – how are terrorists or nation states most likely to use commercial AI tools today? And do we have the right policy apparatus in place to deal with this?

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

SISKIND: Yeah, thank you for the question. Yes, I study the scary end of the AI use spectrum. And often, the highly newsworthy part of it where you hear about like – well, as we as a country are struggling to figure out how to operationalize AI and how to diffuse it across our government.

Terrorist groups, non-state actors, and authoritarian governments are in some ways much better at sprinting out ahead of us and being very experimental. So, you have everything from – like there was a great report this summer that came out about how Boko Haram is integrating AI into their strategy, using it for attack planning and weapons troubleshooting, and designing explosive – and the design of explosive devices.

A couple, I think last month, Anthropic released their AI misuse report, which detailed how the Houthis were using it both for – they're using it basically as a software engineering team. They use it to develop guidance, navigation and control software for guided rockets and multi-stage ballistic missiles.

But the interesting role for me is that the role that ISIS is playing. They're out working with different groups as kind of like a coach and a teacher of how to use AI. They're kind of acting like the Accenture coming into government agencies and getting them to adopt new technologies quickly. So, they're doing trainings and putting out guidance on how to do it.

But then also you have lone wolf actors, like even within America, using AI to conduct terrorist attacks. Last year, there was a bombing of a Cybertruck in Las Vegas and that guy used ChatGPT to plan that attack.

So, a lot of, you know, really scary experimentation on the AI front from terrorist organizations, non-state actors. But in general, you know, a big area of our focus is just authoritarian governments in general, so we're looking at how Iran, Russia, China, Qatar, Turkey and others are using AI.

And there's kind of four main categories that we kind of bucket their uses into. So, the first is just domestic control. This is everything from using AI for facial recognition technology, using it to surveil their population, and any sort of using it in any way possible to kind of hinder the capabilities of journalists or political activists.

Another major category is influencing other countries. So, this could be running influence operations, tampering with their elections, trying to influence their elections, even economic market manipulation.

They weaponize AI tools. So, this might be, you know, advancing or creating more advanced capabilities for existing technology, like using – taking drones and then using them and like creating swarms, or just using AI to kind of amplify their capabilities.

And lastly, they exploit AI systems themselves. So, that is looking at how to gain the most advantage from them. So, that could be anything from the Chinese stealing our intellectual property, using this process called distillation, where they're basically fraudulently creating all these accounts to kind of steal the outputs of the models that they use to then train their less sophisticated models. And that enables them to kind of leapfrog the development process.

You have that. You have the Russians doing data poisoning, model grooming. There are so many different types. They're all – and then insider threat, of course, is another important tactic. So, there are a lot of different ways that authoritarian governments are trying to attack AI systems themselves.

MONTGOMERY: You know, I think we've already seen that authoritarian – I mean, that insider threat by China where – I mean, there's a reasonable reporting of theft of frontier lab intellectual property and transportation back to China. So, that's a great final point.

All right. Ike, like me, you grew up driving surface ships, you commanded the good ship Ramage, a destroyer. You then spent about a decade in the Pentagon working China issues. Where do you think AI is most likely to change the fight between the U.S. and China? And what happens to the side that develops more slowly?

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

HARRIS: I think we're sort of at the beginning of what this looks like, right? So, the same way that, you know, when the internal combustion engine was first created, cars looked like horse-drawn carriages just with the engine in the front, because we didn't understand how to make a car in the way that you'd actually make a car because you didn't need a horse anymore.

We're kind of at that same stage with the military use of AI. We haven't really, you know, we're kind of sprinkling AI onto the things we already do, which is fantastic.

And there's a lot of, you know, to your point, Megan, there's a lot of things we can get out of that. There's a lot of efficiency gains we're going to have. You know, it's going to certainly improve a lot of the technical processes around designing and creating the capabilities.

But, you know, somebody the other day – a lot of what I've done is focus on, you know, a potential Chinese invasion of Taiwan. You know, I have my own skepticism about the ability to pull off the largest amphibious invasion in history with a bunch of guys that have taken the island.

But if you kind of tweak that a little bit and you say, well, the Chinese have a really good manufacturing capability. They're ahead in robot designs. And if you can get a robot to have AI in it and you don't care, you can just drop endless robots on Taiwan. And all of a sudden, that problem of resupplying your manned force on an isolated island is not really a problem anymore.

So, I mean, there's things like that where we haven't quite put together some of the capabilities and said, hey, what does this look like in a new world, not just how does it look like in the things we already do? There's a lot of the AI safety community is very concerned about what the ability for advanced AI can do with bioweapons.

You know, there's a lot of folks that will tell you that there's not a great control regime around precursors for biological agents. That's certainly something, you know, people are looking at. They're raising that alarm already now.

You know, cyber is already becoming an issue. Obviously, the Hugging Face attack highlighted the fact that these models are extraordinarily capable. We're still finding more and more incidents that kind of almost in a daily trickle now of news stories of new hacks that were going on.

So, the world where you have physical platforms and human beings that, you know, take and seize territory or control lines of communication around the world, that's becoming – it's becoming contested in a way that we haven't figured out how to defend yet. And that capability is moving faster than we've built to manage it while we're trying to also manage those capabilities internally.

I think where most militaries fall down is they are – they lack the imagination in an enterprise level to adopt technology, particularly if they're ahead, adopt technology that is revolutionary in ways that an adversary who's behind is forced to find ways that are novel to use something.

And this is where I think the Chinese will be. They will – they have the ability to surprise us in ways they're adopting it, because they're just good at making the best out of a constrained situation. And I'm concerned right now that our military is not being imaginative enough in how that's going to happen and could very well be surprised.

MONTGOMERY: Yeah, I worry. I think I'm more optimistic than you. You know, you and I both, you know, been involved with Aegis. I've been involved for 40 years. You've been involved for 30 years. You know, it's got AI in it.

(CROSSTALK)

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

HARRIS: Right. Had in it.

MONTGOMERY: It's had AI in it since the beginning, almost. Not, you know, at least it's had really advanced machine learning and we've benefited from it.

I mean, Aegis is the combat system for our destroyers you know, how we defend our ships at sea. Aegis has had 800 weapons fired at it by the Houthis and by the Iranians over the last three years and zero have hit our ships. It's a uniquely successful weapon.

And I think one of the things I'm finding really interesting is like – I've told this story before. But when you and I were junior officers, you know, we got an Aegis update once a year. It was like a Christmas present. We opened it up.

(LAUGHTER)

Everybody's excited, you know. You took the testing on the ship, you took the ship out to sea just for that, brought it back and everybody's excited.

Then when I was an admiral, it was about once a quarter when you were commanding a ship. My son's ship now, it's once every three or four days. And I think that's this – what's happening is AI and machine learning, we've put them into – we've allowed them to – I don't say run free, but to start to stretch their legs in a way we never did because we really constrained the system before and had extreme human control.

And now we've got a little bit more going on where we're learning from missile shots and getting it right. So, I can see some of what Megan was talking about, these iterative changes coming. And we've got to let that go loose because to my mind, once we have something like that happening, the Chinese will be watching it, and they'll attempt to replicate it. So, we have to take full advantage.

So, I think there's opportunity. The services have the ability to do what I just described. I think the Navy uniquely has the investments in a place called Dahlgren and some missile defense money that made that happen. But as we start to do that, all of our weapon systems are going to become more effective.

HARRIS: Yeah. If I could just add to that, I think the challenge for the military is that it's essentially right now living off of a commercial ecosystem that is not designed to handle the stressors, the lethal, I mean literally, life and death decisions that are made in the military all the time. And we're not even talking about like the use of force. There's a lot of things adjacent to that.

MONTGOMERY: And we're not heading into the Anthropic discussion here. Okay, thanks.

HARRIS: No. But, so the point, though, that the – how do you maintain the human control and human understanding of these decisions, which are essentially just stacked probabilities that are happening hundreds of times inside of an answer that all look really believable while also preserving the innovation.

But giving that commander, the CEO of the ship, if FCA2 comes up, it's like, "Captain, I just rewrote the code for Aegis, we're going to be way better." And the captain's like, "Make it happen." If that goes wrong, that's the end of the captain's job, right? So – and maybe the end of the ship.

So, how do you preserve the innovation with the control in a way that you kind of you get the best, but don't put yourself on that fire?

MONTGOMERY: And I'm not going to say the military has got everything right, but in that one weapon system and that one service right now, we have it right. And I think it's a model that should be looked at. Now, it was an expensive model funded by decades of, you know, missile defense agency and Navy funding.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

(CROSSTALK)

HARRIS: Took four years.

MONTGOMERY: But I get it. And sometimes that's just glossed over. You know, there's a, "AI showed up three years ago." That's not the truth in the military. The military's had it for a long time, how we've controlled it.

And one last thing I say about this, as you and I sat in hundreds of hours of doctrine review boards on every ship in the Navy, just tens of thousands of hours a year to assert human control over the product in a way that I don't think we have time to do anymore.

This is what we're going to, you know, in addition to moving arrows on PowerPoints, I think we have real opportunity there. So, I'm excited about that. And that's not what you hear the military talk about when they talk about AI. But it's what the military ought to be investing in to make sure we get the maximum out of it and let our warfighters and our systems operate to their maximum efficiency.

All right. Megan, you've written a whole paper on this. I want you to walk us through an analogy you use.

You place AI in the same category as, like, game-changing technologies, like electricity, the steam engine, the computer, kind of these general-purpose technologies that changed everything, but their strategic value only came out when we figured out how to spread them.

You know, and you could see that from where ARPA [Advanced Research Projects Agency] was and DARPA [Defense Advanced Research Projects Agency] was with 10 universities, you know, with the computer for the first five years, to where it is now, where it's ubiquitous in our society.

What – in those, kind of, revolutions, it was diffusion that mattered, that distribution. What's that tell us about the state of AI today and where it's heading in the military?

HAINLINE: Yes. So, general-purpose technologies in general kind of have some characteristics when you look at the research that gets into innovation and GPTs [General Purpose Technology].

One, they're pervasive, so they affect multiple sectors of society. Two, they are improving over time, so it's a continual improvement. Three, they spawn spin-off technologies and innovations in other sectors, so a whole bunch of things could be rooted in conventional electricity and all the use cases that it has. And then, finally, it's got long-term and permanent impacts to society and to the world.

And so, a couple of factors come out of that. One, the long duration that it can take, which you mentioned, to really sink in and have serious impacts across society.

For example, electricity. So, Edison invented the incandescent bulb in 1879. 1881, there were transformer stations in London and New York. 10 years later, only 3 percent of households in the United States were electrified. 20 years later, it was only 50 percent.

So, it just takes time for this infrastructure to build out, and there's a – almost a J-curve where productivity can decrease a bit as that infrastructure, and as you're rewickering your process around using this new technology, you're not using, you know, oil lamps anymore, you're using electricity. It just takes time and you might not see that immediate impact right away.

Same thing for the computers. They invented silicon microprocessors and the 1043-byte chips in 18 – or excuse me, 1969, 1970. 1990, only 10 percent of business enterprises were using computers, and only 2 percent of our business data was digitized.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

So then, an explosion happened. So, you have this lull while the technology diffuses, and then an explosion in use.

And we could argue that with AI, we are approaching that explosion in use. Like, we've kind of mentioned, we've been seeing this technology for a while now. It's not brand new.

The three kind of pillars of what AI needs: data, compute, which could be cloud compute, and then algorithms. The data in the algorithms and quality data, really, and the quality of the algorithms is kind of hard to quantify, but the compute power, we can.

In 2006 was when Amazon Web Service became commercially available. 2010 was when Microsoft Azure became available. So, cloud compute really became available about 20 years ago, and now we are seeing this massive increase.

So, algorithms, as they were trained between 2012 and 2018, increased 10x the data that they were trained on every single year, and that's only increased. So, we are at this tipping point where you really are going to see a lot of AI uses, and that's why we've seen so much technology advancement in the last couple of years.

But what – getting back to the GPTs and how they are wielded successfully, looking at historical examples, like the Industrial Revolution in Britain.

The factors that made societies that really benefited from those technologies are education across their society. So, people that could take that technology, understand it, and then apply it to their own situation, and really use it in their daily life, re-imagine their process, redo things.

Organizations that encouraged the innovation and the use of that technology. So, think in militaries, as the Germans had the mechanized infantry – or mechanized armor divisions, the tanks became a thing. They took real-world exercises and they re-imagined their entire structure of their military.

The French also had tanks on par with what the Germans had going into World War II. The Germans developed the blitzkrieg because they re-imagined what their organizations would look like. They didn't keep them in the same constrained type of command structure that the French did. They completely revamped it, recognizing this is a fundamental change to their technology.

And then, finally, resourcing that technology. So, you have to, like, build up the infrastructure around it, and for AI, that is, again, your data, your compute power, and then your expertise, you know, the personnel behind it, they know how to use it, so.

MONTGOMERY: You make me nervous there when you anchored it in education, because if – there's one thing that I think we're slipping here, and our immigration policies are really negatively impacting, its education and the quality of our PhD students and what happens to them when they graduate.

So, hopefully, we can – the Department of Defense or the Department of War will turn its eyes on correcting the White House's immigration policy. No need to comment on that.

Hey, that was a really interesting thing you had said there about how the militaries were involved, the innovation in the military, because that leads to my assumption that, you know, whoever gets the technology first wins. But – and, you know, you've laid out before that history kind of complicates that.

What does the record of past military innovations tell you about the source of advantage? Is there a cautionary tale there for the Department of War on how we use AI?

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

HAINLINE: Definitely. And again, there's a great quote by James Mattis, the 26th Secretary of Defense. "Success doesn't go to the country that develops a new technology first, but the one that more swiftly adapts its way of fighting and integrates it into its military." And that won't be word for word, so don't quote me on that. But it's along those lines.

That quote is actually on the entryway into the operational test squadron for fighters in the Air Force at Nellis, where I spent three and a half years. So, our job there was, we get a new widget, it's been approved by developmental tests. It's not going to shake off the airplane. It's a new sensor. It's a new weapon. And then how do we actually integrate that into our way of fighting? What does it do to fundamentally change our processes, our assumptions behind everything that we're doing?

And there's a ton of historical examples of this. Again, the French, they had the same tanks or better than the Germans, didn't look at it hard enough and come up with this operational concept revolution that changed their way of fighting.

Same thing with the French Navy in the 1800s. They had the first steel hull warship, first steam powered warship, first mechanically operated submarine. They didn't nail it against the Brits and, later, the Germans. And so, a lot of that was infighting in France at the time, political fighting about, are we a deepwater, high seas Navy that focuses on battleships, or are we a flotilla type coastal defense Navy?

And so, if you can't agree on or determine the best way of using that technology and what your force is meant to do, then it's really difficult to take advantage of that, even if you just have the technology. You haven't revamped your processes around it. But yes.

MONTGOMERY: Well, Admiral [Will] Metts and I appreciate your reference to General Jim Mattis in that comment. But you're right. He said that as Secretary.

Hey, Ike, you had a front row seat on the China Select Committee to how the CCP is, generally, trying to integrate AI into its military and security apparatuses. What are they doing that we should worry about most, and where is the Western picture of what China is? Where do we see them as 10 feet tall when they're not?

HARRIS: Yes. I think the – their strength is going to be adoption, kind of the point you just made. Their system is just far more risk tolerant for things going bad if they're going bad in the pursuit of a kind of party goal.

They're not nearly – I mean, if – you can go look up on Twitter, once every month or so there's a – excuse me, X – once every month or so there's a Chinese solid rocket motor booster that falls on a village when they launch a satellite. I mean, it's not like, oh, this happened one time. It happens, like, as a regular thing. They just don't have the same concerns that we do.

I think if – you know, if Elon dropped a booster on Daytona Beach, I have a feeling SpaceX wouldn't be around for a lot longer.

So, if that's your framework – like, I can kill a village with a rocket booster if I'm pursuing my space program. Like, what does it matter if I, you know, have a couple of things that go bad in a ship or an airplane, or a missile? Like, I'm experimenting. I'm at the edge. I'm doing cool stuff with it.

I think the biggest problem between our two systems right now is our military is mostly using U.S. AI, which is, for the most part, done through an API [Application Programming Interface], so you have to have, you know, excellent bandwidth and connectivity to a data center. You don't put this on a platform. You have to have the connectivity.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

And in peacetime, that can happen right now pretty much anywhere in the globe. However, you go to war, and all of a sudden, as the Ukrainians are finding out, you're not going to have the ability to have – to send and receive electromagnetic radiation, and therefore your communication can be shut off, and basically what's on the device is going to be it.

The Chinese system is all downloadable, small model weights. That's what – that's they've specialized in. They're doing this through distillation and stolen chips, and all sort of stuff. But they're getting capability that is near frontier level, but you can put it on a laptop and use it.

That system is going to be far more transferable to the military, especially, you know, in austere environments where platforms are operating in consonant environments or don't have the – you know, in a stealth capacity where they can't transmit. That's going to be far more useful to them.

And I am concerned that without an open weight, or, at least, downloadable model that can exist on a platform in the United States right now, that they're going to have an edge on putting this onto the platforms at the edge and finding out ways you can use them that, right now, our system just doesn't allow.

MONTGOMERY: So, I love that. You can either destroy a village or raise a village, I guess. That's the Chinese versus American approach there. All right.

Hey, Megan. One of the central distinctions kind – that you lay out between building AI programs is – between building AI programs and building AI competent or enabled workforce. What's the difference in practice? What's it take to make AI literacy part of a professional competency, particularly in the military?

HAINLINE: Definitely. So, we, again, focus a lot, and there's a lot of announcements around these big projects that are led by some central organization, CDAO [Chief Digital and Artificial Intelligence Office] or the DRPM-UxS [Direct Reporting Portfolio Manager for Unmanned Systems], that are focused on a drone or on a specific technology.

But, to do a whole workforce that's enabled by this and is thinking about it actively as a part of their own job, you need education. So, people need to understand the technology and imagine its use cases, both its strengths and – strengths and weaknesses in the application to their own job.

You need to resource it, as in, with talent available, so we can go vibe code something. But if you don't have an actual professional there to tell you where you've gone wrong or where this is now breaking rules, probably not a good idea to just unleash whatever you came up with for your process.

And then, you need the organization structures that encourage that as well, so allowing people to rethink their process. And if it's not their part of it that is the problem, allowing them to go up a level and, like, hey, the whole process at the entire base level we need to think about. So, it's kind of all three and they're reinforcing.

So, talking about, you know, not having a technician recode Aegis and then have an issue, you need safe to fail experimentation. So, you have to have local encouragement where people are allowed to experiment, but in a way that is given frameworks, given safety constraints, so they don't go do something unintentionally, and then the environment to go test it out and to try it.

So, like naval gunnery competitions. You know, who is the best at this? You guys can try any way you want. It's not a big deal. It's not combat. Right now, if you miss the target that you're trying to hit, but now we can narrow down on what is the best use case for this.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

So, you need to actively be experimenting with these new processes, with these new technologies. And then also have that feedback mechanism in place for your organization to find the best use cases for it and pass those lessons learned so we don't have to just relearn at every location.

MONTGOMERY: Yeah, that's interesting to hear you talk. And I get that the – careful how I say this – the fighter pilot mentality versus the kind of like technician mentality. I worry about this.

If you change a component in a weapon, either software or hardware, currently it puts it back into a 12-to-18-month assessment cycle, testing cycle, validation cycle, that happens first in a lab, then in a ground-based simulator, then up in the air. And I worry that, you know, we've – it's going to be very hard to draw these lines.

When does modifying something or allowing AI to modify something put you back into a dramatic review cycle? And for aviators, this is written in blood, right? The desire to take it back is – most of our NATOPS [Naval Air Training and Operating Procedures Standardization] manual for the Navy is written in, we killed somebody doing X, so we're not going to do X anymore.

Then we figure out another way around it. So, this is going to be really hard. I think it's going to be much harder than it sounds. You know, I remember my wife used to – she was a helicopter pilot, and they would used to get their gun calibrated, they'd use little X grease mark spots on the lower windscreen. That I think you can do. You're walking the – up an arc like that because you're not changing the weapon system itself.

But if you start to go into the weapon system and say, "I want you to fire a little higher, you know, by some kind of software or hardware change," it's probably going to kick it back into a cycle. I think that's going to become really, it's going to become very hard for us very quickly if we're not careful.

HAINLINE: Agreed. And I think our testing processes need to accelerate, and technology can help with that, as I kind of mentioned before. But there's certainly a range of peacetime innovation, the speed at which you test things, the speed at which you're allowing people to change things, and wartime.

I think we really see this in Ukraine with their drone operators, and they are at the point where a lot of people in those units are technology experts, and they go in and recode the algorithm and do that on the fly and then pass back up those lessons, but it can't always go well.

(CROSSTALK)

MONTGOMERY: It doesn't.

HAINLINE: So, we're not there. Obviously, like, that is not what the US is in our operations. It's what no other nation really is in, in that type of environment where it is immediate life or death. You're in combat and have to do that.

But we are also in a period of very high competition and very fast-moving technology, so we're not where we were 15 years ago either. And we need to find a way to transition into a more rapid testing, allow in the field testing in safe environments where it is, you know, workable and where it can be controlled.

But there's got to be kind of an in-between, and we have to shift away from the long-term acquisition, which is happening with a lot of initiatives that we've got.

HARRIS: Mark, I...

MONTGOMERY: Yeah, go ahead.

HARRIS: ...So, I think, you know, we always go to the where's the edge of lethality and, like, how are we going to fix that or make it better or more efficient, whatever.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

One of the things that we've been thinking about is, you know, how do you just put an agent on a system like Aegis and just advise. You know, collect data, collect patterns of human behavior, things that right now, you know, one guy that gets certified out of the school with that, you know, in the Navy calls it NAC [Navy Advancement Center], that guy can sit that watch once he's, you know, passed qualifications. And he is exactly like the next guy other than maybe some, you know, some hard-to-define characteristics.

Well, if you have an agent sitting on that watch station, you can actually get a pretty good idea what that guy does, because you have a granularity on his actions that you would never get as even a, you know, a subject matter expert sitting over his shoulder watching to train.

So, I mean, there are things where you can start to augment the human behavior without taking the human decision out of the loop. Things that we just have, you know, kind of hand waved is we'll never get there because it's too hard to measure. Well, if you have the system behind you, those things are now, become measurable.

MONTGOMERY: Yeah, I agree with that. I – back what you're saying on Ukraine. I have to say, I see a lot of things happen in Ukraine with this modern, you know, this technical adaptability, adaptation, warfighting they're doing, which every – not infrequently accidentally kill Ukrainians in a way that makes us uncomfortable.

I mean, we're a country that just spent \$350 million rescuing one pilot. I mean, we go to an extreme, and it was an Eagle. I mean, who knows? But the – that's an Air Force pilot joke.

But, and, you know, we don't – one of the reasons that we got our butt kicked in the war with Iran in terms of ground-based drone defense was we're unwilling to integrate weapon systems. We're unwilling to fire weapon systems that were not integrated into the broader warfighting like Link 16 and other systems for fear of hitting our own pilots, which is not a – not – is a serious issue.

But all that's going to have to, you know, there's, I think everything's going to be in play in this. How we think about this; how we take risk with software changes, hardware changes. Because if you have something other than a detailed technical environment, testing it and retesting it, it's going to get risky.

So, I'm excited to see where this heads, but I also think it's, it's probably a lot harder than some of the line officers think and the engineers know. So, it's going to be interesting.

All right, Leah, we've done a ton of DoD stuff here. Let's bring it back out. You came; we were lucky to get you here at FDD from the Department of Homeland Security when they defenestrated themselves.

(LAUGHTER)

You were the deputy director of the AI Corps. And before that, you led tech modernization efforts at the White House for four years. This administration's really asking, you know, really taking a really aggressive top-down approach to promoting AI across the government.

But innovation in government can sometimes be a really challenging – I mean, if we think innovation in the military is hard, it's even harder in the government, I think. And much of the government isn't necessarily really AI ready or equipped or have the talents right throughout them. How can pushing AI, you know, from the top-down work and how can it backfire?

SISKIND: It's very interesting to see how the Pentagon is approaching AI, and some of the lessons are great and should be applied to the rest of the federal government and others definitely give me pause.

Any opportunity we have to, you know, get into a heavily bureaucratic environment and make things just work faster and better for the public is great. When I first heard Megan speaking about her area of research at an event last year, I was so excited because it was just a topic that no one was hitting on.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

Like, how do you get – how do you get into the real, really boring admin, bureaucratic stuff that, that people don't invest enough time in figuring out how to streamline? Because that's where you can really make major efficiencies and gains. And when it comes to public facing services, when you can make technology work for the public, it has huge ramifications.

This is when a person can navigate a government service relatively easily without that much effort, that makes you – that makes you have more confidence and trust in your government and in democratic institutions in general.

So, when something as minor as like, if a website is kind of glitchy, it's worth investing in that kind of thing because it has huge impact on the public and how they perceive their own government. DoD's approach to AI has been very interesting. They've taken a lot of bold moves in kind of lowering the hurdles in procurement for AI tools.

So last summer, they made really interesting move to kind of place bets across four different AI companies, equal bets, and to see who was going to, you know, without placing favorites, and just see who was going to proceed the fastest and be cleared for classified systems. That I think that was a really great approach. It's kind of like what they did in Trump one with Operation Warp Speed. So, it's been very interesting to see how they've all progressed.

That being said, I think the intense cultural pressure coming from the top down of, "Use AI!" And we're, you know, putting out like AI slop post that says, you know, "We're an AI first workforce," is a lot. Because leading technical transformation in government, it's often largely a cultural process. You have to get people to trust the tools that they're using, and you have to get them comfortable with this.

And we're at a moment in time where the public does not have a lot of trust. In fact, I would say trust in AI is waning. There have been polls that this summer – there's been so many, so many new stories that I think have kind of diminished the public's trust in AI.

We're seeing – well, I won't get into loss control issues yet. But we're seeing a lot of activities that rightfully give people pause. Also, another issue with pushing AI use from the top down, that doesn't mean that the government and all of our systems are necessarily AI ready.

So, we have to deal with the underlying problems that we have. Data being siloed, or maybe not necessarily the highest quality or accessible. You have to address these issues first. And my biggest concern with kind of the pace that we're adopting AI is it's actually going to expedite bad processes.

Like when I was with the U.S. Digital Service, a lot of what we did was looking at like, let's look at a process end to end and figure out how much of this bureaucracy is really necessary? Can we figure out ways to improve it? The problem with AI is it makes things so fast, that it will make it easier to have bad processes just run a lot faster. So that's a top – that's one of my primary concerns for government AI use.

MONTGOMERY: Thanks, and you mentioned Megan's initial brief she gave when she was with us. You know, in that you laid out your three pillars on education, organization, and resourcing.

But AI kind of runs on data. And DoD data is notoriously fragmented by both classification and organizational constructs. It could get locked in silos really easily intentionally. I'm not sure I've seen an adaptation strategy or an adoption strategy for this that really gets at it. What can the Pentagon do here to kind of address this problem?

HAINLINE: So again, I think that's where looking at your process, like exactly what Leah was just pointing out. Not automating a bad process but getting the people that understand the technology in the room with the users who are trying to accomplish a task, your warfighters, and reimagining. Take a whiteboard, sketch out, "Hey, if we could remove some of these barriers, or if we could do this more easily, how would we do it in a logical fashion? And how would we rebuild this process in a way that makes sense?"

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

And so, discovering those little choke points where your systems don't talk to each other or your encryption breaks down or only certain agencies have access and they're on, you know, an Excel sheet saved on a shared drive instead of having that available to people.

It's really about getting the conversation at the right level of the organization that controls that process. So, you can completely reimagine it not just your little end use case. Like if your output for a process is you have to send up an email with an attachment of a PDF or an Excel or something to another organization, there's only so much you can do to use AI to fix that. You have to get the actual work and the AI application at the right level so that the whole process can be reimaged. And that's how you start to break down those siloes, these inconsistencies across services and organizations.

So that's why a multi-tiered approach of having people that understand the technology, that are educated on it, get its strengths and weaknesses at every level, and are open to re-imagining their process. They recognize there's a problem, and then they have access to expertise that can help them rebuild it and sketch out what right should look like.

That's why all three are really critical at every tier of the organization.

MONTGOMERY: You know, you didn't argue for it, but the President takes your thought and says, "Hey, I'm going to create an AI Force." So, Leah, how realistic is an AI force? And at DHS, you were at the AI Corps, which is – clearly is different than an AI Force, I guess. But they – the kind of talent pipeline that the – Megan argues that DoD needs, what do you think, from your experience at DHS or watching the DoD, what kind of workforce ideas are going to work? What aren't? And if we really did try to stand up an AI Force, any kind of recommendations?

SISKIND: Yes, lots. Well, first of all, this was just a tweet – and I still say "tweets", by the way, and Twitter – but this was just a tweet of his, so I don't know how serious it is. But ultimately, I do think it's a good idea because no matter what, whether you're a doomer or accelerationist, one thing that we can all agree on is that you have to have top-tier AI talent in the federal government. You need them overseeing procurement. You need them advising on cybersecurity issues. Just no matter what, the federal government has a huge role to play in AI use and governance, and it's critical to have top-tier talent in government.

It is – there are major challenges in getting talent in the government. You have pay issues. A lot of the country's technical talent is in California. They don't want to necessarily be in Washington, D.C. And then you have to deal with a bunch of bureaucracy and process which sucks, as we've been talking about. So, it's totally different environment than working in a lab.

But we have done this before. We have figured out how to do this. And ultimately, a lot of really, really smart people are most motivated by the mission, and they want to find other ways to serve their country. And so, if you sell – if you come to people with an incredible mission, which is not hard to find in the federal government – all of the different areas that the work touches on – you are able to get really good talent.

We know the pathways to do this. You can –there's a lot of – there's kind of, like, a playbook to follow. Unfortunately, all of the people who developed and ran this playbook were effectively pushed out by DOGE last year. So, this is organizations like mine, the U.S. Digital Service and the DHS AI Corps, other great technical units like 18F, the Presidential Innovation Fellows. I could go on forever. Like, we had a lot of excellent talent, and we can do this again.

But you do things like meet the talent where they are. Not everyone wants to work in Washington, D.C. That's OK. Let them work in Silicon Valley. Or you create special pay scales for this kind of rare talent.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

You are – and one of the most important things is you have people embedded in agencies who are constantly scoping projects so that you can quickly slot in tech talent that – because the average person who works in tech, they don't have a long tenure anywhere. Like, in government, it would typically be, like, 18 months. So, if you were just on your own, it would take you that long to get your laptop and, like, your ID and stuff like that.

So having people embedded already who can help scope projects, keep the work moving, and help, like, guide people through that bureaucracy is very helpful. So, we know how to do it, we can do it. We should do it again.

MONTGOMERY: And I do think it started out as a Truth Social post, but the...

SISKIND: Oh, sorry.

MONTGOMERY: But I'll also remind you, the Space Force started out as a tweet. So, you know, I'll take my prerogative here for a minute and say, you know, if the President had the wherewithal to establish a Cyber Force, he'd be in a pretty easy position to slide in an AI component to it.

But without that, without a military – there's no element of the military that considers itself 50 – no service that says 50 percent civilian's OK. You know, we're all about 90 and – you go on a Navy ship, there is 275 service members and one or two civilians. Army battalion, an even tighter ratio. Air Force squadron, Navy fighters – plane squadron's a little different. There's a few more black box workers. You know, civilians that are contractors that are with the squadrons.

But cyber and AI, this is something I could easily see the force being 50-percent civilian or more. And a – as I've said for cyber, they can be, you know, face tattoos, fat and smoked a lot of weed in high school, and we don't care. As long as you're the right guy, you know, or man or woman for that – for that technical application.

All right, Leah, I want to stick with you for a second. Some of the AI – can't – speaking of people who smoked a lot of weed in high school, some of the AI contractors for DoD, like OpenAI, have recently come under fire for attempting to attack the actual governments they are supposed to serve or the corporations they're supposed to serve.

On the one hand, we're trying to leverage AI to turbo-charge our military, but on the other hand, we're seriously worried about losing control of these tools. So, it's – I think it's time to talk a little bit about loss of control, and we'll talk about us and then in a minute about China.

But how do we hold both of these realities at once, that we want this help, that they're supposed to protect us, but we're also losing control over them?

SISKIND: Yeah. This is a – I don't know if there's any historical precedent for something like this. But it is what appears to me to be a totally unprecedented moment in history, where the – yes, the technology that we're using is so important and is so critical to many of our government functions, and yet we are at a point where we are realistically – like, we were really grappling with loss of control incidents.

Ike mentioned the Hugging Face incident this summer, which was OpenAI running a test – a security test on a model that was not publicly available, and they found out that, without their direction, that their agents autonomously went rogue and hacked another company called Hugging Face.

Since then, more developments have emerged from that same security testing, and it appears that they have also inadvertently hacked the Australian government, their Medicare system, which the Australian government is not happy about.

And in America, the – they found that they've – hacked – well, the wording here is very, very important. They have targeted and exhibited strange behavior around the Census Bureau website, and there was a genuine attempt to hack the Department of Education.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

By the way, it's very interesting to see how these events are being reported. I think the media wants to tone down the heat on this because if a human did what these agents were doing and just stumbled across access keys and then used them to log into a government website, not for the purpose of then disclosing that vulnerability to the government, we would call that hacking.

So, this is a very scary moment. These agents are searching for data, they're using – they're – to answer questions in security tests. But they are showing that they – you know, you give them an end goal, and they are using whatever method they can to accomplish that goal, and it's quite unpredictable.

They – yeah, it – we're reaching a point where we just don't know what they're doing. We don't know what they're capable of doing. And testing is – it's getting harder and harder.

MONTGOMERY: Thanks. So, like, you run one of the few, you know, non-profits that has really taken a detailed look at this AI safety issue. What – how does the approach to AI safety differ that you see in the United States from the one you see developing in China?

HARRIS: I mean, I think it really starts with the, you know, quite stark differences between Chinese and U.S. society. You know, you cannot – you don't have a sort of segment of Chinese society that decides that it wants to make a vocal, you know, campaign and lobby, you know, the politburo about an issue that the government clearly says you can't talk about.

You know, our administration is – you know, the President has been very clear that he is not on the side of, you know, major guardrails or new regulation or laws. If, you know, if Xi Jinping came out and said that that would be the end of the AI safety discussion in the Chinese Communist Party and the country overall.

However, they have a – you know, the party is concerned about the party's control. Loss of control for anything, be it AI or, you know, a dissident movement, is equally as dangerous to them. So, they have started to talk about loss of control in some of their authoritative documents on AI.

There was a framework – I can't remember the full title of it. It was, like, Framework 3.0 that came out, I think, September 16th, give or take, that actually, for the first time, mentioned this sort of loss of control-like language. It was actually printed in English and Mandarin, and that was fairly consistent in the translation, which was interesting in and of itself.

But they discussed in there that, hey, this is a potential problem that we'll have to deal with. However, they put that below, you know, the societal benefit from AI, which they firmly believe AI is going to carry them over this, you know, demographic cliff they're about to encounter, and all of the economic impact that's going to have.

So, they see AI as the thing that is going to generate, you know, economic and national power while their country is basically shrinking by, you know, significant numbers over the next 50 years. Anything that happens with AI sits below that concern, right?

So, this is – you know, there was a lot of discussion in the media and parts of the country around what was going to happen in this He Lifeng/Treasury – second – Treasury Secretary Bessent meeting, and then ultimately Xi Jinping and President Trump.

And I think they both kind of got to where they both were willing to go, which was, "Hey, this is a problem. We should continue to talk about it. Neither one of us is really on a page where we're going to agree to some kind of resolution or a, you know, guardrail or system that would allow the two countries to manage this together."

This is a competition. Both sides see it that way, and it will be that way for a long time.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

MONTGOMERY: You know, that's a – you remind me of – the president was really direct that he not going to let China beat us, right? He's said that multiple times. And I find the kind of – the hypocrisy between "I'm not going to let them beat us" and then he turns around to Taiwan, the country that is going to allow us to win. I mean, to be clear, we get 100 percent of our AI chips, not 94, not 99, 100 percent of our AI chips from Taiwan. And even chips that we build here that are just below the ones for AI usage still have to go back to Taiwan for packaging to come back to us.

So, I mean, this is a – you know, I – over the next half-decade, it's going to become increasingly clear to even the most, you know, narrow-minded Americans that Taiwan's the most important country in the world to our economic prosperity. And you cannot simultaneously say, "I'm not going to let China beat us" and not turn and say, "I'm going to do everything possible to keep China inside, you know, the democracy – you know, the list of democracies we fight to protect." But I think this president on occasion fails to make that connection.

Look, sticking with you, Ike, are there any – after that the destruction of the U.S.-China relationship I just did, are there any shared concerns within the U.S. and China that you see are realistic opportunities for collaboration here?

HARRIS: Yeah, I think there. And, you know, as we talked about earlier, they're, you know, terrorism and/or terrorists and organized crime like this is going to continue to be a problem. We're going to see greater and greater sophistication of attacks.

I was at a brief while I was on the Committee from a major cybersecurity company that was actually saying that they're not seeing, you know, cyber hacking through like code or trying to break it a break – break – break into bank accounts is the major problem.

It's the fact that now, you know, somebody in a Triad gang in like Vietnam or something can now call your grandmother. And after they've scrubbed your social media page, tell, you know, grandma that little Johnny's in the hospital. And if she can't transfer \$20,000 to pay his bill right now, he's going to – that he's going to die or something.

Like that level of sophistication because you can, you know, AI can speak in a entirely believable American, you know, local regional accent. And the translation factor of the Nigerian Prince with the broken English sending me an email about how I need – he needs my help to transfer a million dollars, that's gone.

The sophistication these attacks is going to get a lot, a lot worse. The Chinese see that as a problem just as much as we do. They have their own adversaries that they're concerned about using these things.

I think there is a lot of room for both sides to talk – to start to define what AI risks really mean as, you know, as we did with nuclear risk. Like there are things where we say this is a red line if you do, you know, if we see a Chinese AI agent trying to take down the U.S. stock market or going after Bank of America.

That's going to be a problem and we're going to respond to that if we can attribute it. That's a good thing to articulate to your adversary, that you don't need to have any kind of agreement in place to make sure they understand.

MONTGOMERY: So, you're saying China's going to take AI to eliminate Winnie the Pooh from the global Internet?

HARRIS: Stranger things have happened.

MONTGOMERY: All right. Let's see. We got a few minutes left. Before I let Megan wrap, I'd see if we have any questions in the audience. Anybody have a question? There we go in the back right there.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

SHELDON: Thank you for the presentation. That was excellent. I have a question for you on the far left. You mentioned the DOGE cuts and how that was sort of a challenging moment, but do you think there was a positive side consequence that maybe a lot of these people who had all these innovative ideas who couldn't actually get through the bureaucracy that they were currently in got pushed into other sectors – in the private sector most notably, and actually are making significant changes?

SISKIND: Thank you for the question. And just a caveat, I would not classify myself as on the far-left.

(LAUGHTER)

But thank you for asking. I, actually, I do feel like there is a one clear strong silver lining of the DOGE cuts, which is the best tech talent of the federal government has just dispersed across the states. And that in the states were always under-resourced and, you know, struggled to attract that talent, and now is their moment.

And if you look at what Maryland and Colorado and California and Virginia are doing, they are doing incredible things. And anyone who knows, who follows AI regulation, the most interesting things are happening at the state level right now anyways. This is the true laboratory of democracy where every state is taking a different approach and figuring out different things.

So, I'm very happy to see that's happened. I still hope that the federal government can get back to recruiting and attracting the best, you know, talent in the field but for now, I'm really happy that the states are having this opportunity.

MONTGOMERY: If that's the best news out of DOGE – that's like saying the best thing about the great floods of Noah is that we learned to build a big ship.

(LAUGHTER)

Destroyed the rest of society. Okay. I'm sorry, another question over – Mary, you have one or...?

MAHER: Hi, Theresa Maher. I report for *Inside Defense* for Emerging Technologies. Mr. Harris talked about the military struggling to adopt commercial models not built with the military constraints in mind.

The super – the overall like superintelligence accords signed the other day with the top four AI firms in the commercial world. Does that agreement signed like impact the equation at all? Is there anything that anybody on the panel would change to push the kind of merging of commercial? Like the commercial technology kind of considering the military constraints along further?

MONTGOMERY: Go ahead.

HARRIS: I would just say that the, you know, the military – you know, Secretary Hegseth has been very forward leaning on getting AI into the Pentagon, and that is a good thing. The – where we have work to do is there are some very specific constraints, particularly as you get higher and higher degrees of classification on things that are very specific to AI.

You do not have the level of, you know, commercial unclassified compute on JWICS [Joint Worldwide Intelligence Communications System], you know, on the on the highest level of classification – classified networks that you do in the commercial world.

So, if you were trying to move, you know, frontier level platform up to that level of capability and then use it, there's going to be some problems with that. I mean, if anybody's ever been on the, you know, any JWICS site and seen the functionality, it's not great. I mean, it's like the best 1990 software we had to offer.

So, that is a problem that we will have to figure out, you know, what that – I used to do supply chain risk management before I went to the Select Committee. There is a supply chain risk management problem in the AI tech stack.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

If you're not going to clean – there was a report in the journal, *Nature* journal, in May that this group of scientists did a study to look at Chinese propaganda winding up in Western models through just pre-training data. And then that propaganda then causing an alignment toward China inside the Western models.

These were, you know, “Western models.” Right? So, not DeepSeek but, you know, our companies. If that's moving up into, you know, JWICS and then being used to do military planning against the Chinese, I could see that being a problem.

That's where you have to – the DoD has to come in and say – the DoW have to come in and say there are specific standards that we have to adhere to that are different from the commercial world. And if the commercial world is going to do it, how does it actually work?

And, you know, the training continuum of AI, can you do it at pre-training? Is it something that you can do in fine tuning at the end? I don't know. But I think these are the places where DoD really has to – DoW – really has to spend some time and figure out with the companies: how do I make this better for the warfighter? And that's a big problem. That's a big question, I'd say, and its going to take a while to figure out.

MONTGOMERY: You know, I think almost as important as that sign, more important than that signing was yesterday's speech by Secretary Hegseth. And you can throw out a lot of the rhetoric that he gave, but he had some substantive, useful announcements. And one of those, I think the Autonomous Warfare Command initiative is a good one.

I'm not saying a COCOM [Combatant Command] is the first place I would have gone to solve this problem, but we are so broken. We so utterly failed the force in our acquisition programs. There was such an obvious need to be able to shoot down drones, and we didn't do it.

And there was examples, 23-plus examples in Ukraine, you could have taken from and we didn't do it. That the current system has failed. And so the autonomous, to me, the Autonomous Warfare Command, even though the Combatant Command has all these – I have all these nightmares of bureaucracy that will come with it, that will slow it down, it's got to be better than the current system, which is a service-based system that failed.

So, I'm looking – I think he's making the right call there. And I think that will be – it's a different problem than what the president was trying to solve. But I think it'll be more germane to the military than the kind of like the moral authority clauses that they all signed in front of.

HARRIS: And I'll add that I think AI uniquely needs to be aggregated to make it useful, right? Like if we have a situation where every office in, you know, in the Pentagon or in services are buying eight GPUs and then chaining them together and trying to use a model...

MONTGOMERY: You mean AI acquisition?

HARRIS: I mean, the technology itself.

MONTGOMERY: Yeah.

HARRIS: You have to put large numbers of, you know, AI GPUs into one place and get them to run training and to run the models and inference. If you're distributing that by over the entire force in onesies, twosies that eliminates – like you don't get the same disaggregated effect that you do if you put them all together.

Same thing with the talent. Like you don't have enough people to then spread throughout the entire force and put them at lower levels. You have to put that all in one place and get the benefit and then spread from that one place out to the rest of the force.

MONTGOMERY: Thanks. Mary?

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

BROOKS: Thanks so much. This has been an absolutely fascinating conversation. I wanted to see if you could tease out a little bit more on something that all three of you touched on, which is like there's this huge mandate to do AI. And we've talked a lot about individual platforms and programs. We've talked about top tech talent. What's the median look like?

Like for the average logistics officer, for the average military spouse, for the average pilot, midshipman, nurse, contracts officer, how much has AI already changed their experience and how much has it not? Like how much of what we are talking about is on the far edge?

MONTGOMERY: Megan, do you want to go first?

HAINLINE: I will. I'll be honest, I think the answer is a little disappointing. So, you have all these mandates like use GenAI.mil and everything we get is typically lagging because we have to put those safeguards in and make sure it's good for CUI and higher classification systems and doesn't...

MONTGOMERY: CUI being?

HAINLINE: Controlled Unclassified Information. So, there's like information levels and when things start to get classified, it gets much more difficult. And so, again, taking a commercial application that didn't have those guardrails built in, it's just a lag.

That is kind of the premise of why I wrote what I did. And I did this, a professional military education year last year, wrote a paper about it. And that is what I've continued with FDD with this paper we're going to publish.

It is disappointing, honestly. As the end user, you maybe have GenAI.mil. We had just one of the chatbots on there for a while. Just a month or so ago, we got two more. We finally got Grok and OpenAI. But no real push for, hey, go take some courses on how to best utilize an LLM if you're going to use this in daily life. No push for, you know, curated education playlists.

There's a lot of resources out there but actually trickling that into the unit level and having somebody walk you through it and break away from your daily tasks, which take 12-hour days and everybody's very busy. It's hard to take a step back and, you know, get to learn about these new technologies until it is kind of forced upon you.

And that was a large part of the recommendations I make is having a network of get an expert, pick your nerdy coder in every squadron. You always have one of them who's a gamer on the weekends and gets really into computers. They can be your AI expert and give them the authority or the power.

Tell them, "Hey, once a week, send out a newsletter, recommend a couple of courses or videos people could watch if they wanted to learn more about this." Give them a foothold because it is overwhelming. If you're like, "I want to learn about AI," you have no idea where to start.

And that was kind of the transition for me. This past year, I spent at a think-tank here – or a project here in D.C. away from the military, and it was the first time I took a Coursera course. And this was the Special Competitive Studies Project that I was at, they have a Coursera course on just like how does AI work? What are the strengths and weaknesses of it? It takes you through prompt engineering. And I was amazed, and then, also, really disappointed that the military had never encouraged me specifically to do that.

And you can go find these resources. They're out there. We have Coursera licenses. There's – it's not to say that there aren't projects and programs out there in the military and the DoD that encourage this. It just is hard to trickle all the way down to the unit level, and to penetrate your daily process of flail and just doing your current job.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

It's difficult for it to break through that. And that's where you have to have a deliberate, you know, organization structure that starts putting people that are the point of contact to get the foothold in with everybody else in the unit to start to imagine these things.

And then, even if you were to try to come up with a new process, now you need your leadership buy-in, you need access to a talented professional that can come in and take a look at whatever you built and your new idea, and give you the green light and the thumbs up. And then, somebody else to pass that on to two bases over that does the same thing, and their process is also broken.

So, I'd say, right now, not great. I'm hoping to see that accelerate. There are a couple of, like, base commanders I know that have made big initiatives out of this. It's really dependent on the personality, I think.

But I know that the leadership, for example, at Shaw Air Force Base has a whole thing about this and is pushing people to get educated and to start rethinking their processes.

But it's, I think, very spotty at this point. There's not a concentrated effort across the force. There's not a, "Here's the playlist of education things you need to go watch about AI." That's just not quite there yet. It's still a little bit scattered.

MONTGOMERY: One last question over here. Yes, go ahead.

CAMERON: Bill Cameron, retired Navy officer.

I want to pick up right where you left off. I think what you've done a great job here this afternoon is described something we call the revolution of military affairs, right? You have a new technology, you combine it with other technologies, with a new organization, new processes, and you have a military capability several orders of magnitude that we've ever seen before.

But the doctrine and the culture piece is very, very important. You have to get that right. And you described the blitzkrieg tactics that the Germans used. They worked that doctrine up on a gym floor for years before they ever had tanks, as you probably are well aware.

Talking about China and the US, which of these countries is going to have more difficulty culturally and doctrinally with using the new technology?

HARRIS: I would just say the – I think the United States – you know, I like – I love to hear when somebody quotes to me like how many PhDs the Chinese produce. It's like that's the – like, therefore I win. Like, they have five times us per year, like, end of argument.

And then – but somehow, we tend to be in the lead on innovation. So – you know, there's a bit of a – you know – the thing we're worried about that we care about is the actual innovation, right?

The United States has – I mean, you know, maybe comparable to any time – any other time in human history, the most effective capital to idea, smart people, putting them in the right place, and then allowing that person to then create a technology that revolutionizes the world. We've seen it time and time again, and this is just the latest iteration of that.

The Chinese, on the other hand, are locking down their AI executives. They extended that this week to, not just the AI executives, but senior – or more junior people, as well as their families. They're making sure with the Manus, this untangling from Meta, they made sure that anybody in China knows – that everybody in China knows that if they come up with something really cool in AI, they better not start taking any Western funding.

Which, frankly, has been most of the innovation that has come out of China has been at the heels of Western capital and Western know-how.

October 1, 2026

Featuring Major Megan Hainline, CDR (Ret.) Isaac Harris, and Leah Siskind

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Bradley Bowman

So, they are, sort of, in this attempt to lockdown this technology, also, you know, cutting off the golden goose in some – to some extent, because we haven't been able to do it to ourselves.

My hope has always been that the Chinese system will implode faster than our system will win, and I think that this is an example of how that is true. That their entire system is based around control and stopping creativity. That is the secret sauce of America, and this is an example of how we're just going to continue to be better.

MONTGOMERY: Thank you. Yes. That's a great line.

(LAUGHTER)

The – I – you know, I'm glad you mentioned revolution in military affairs. I think when you read – when Megan's paper comes out, you'll see that revolution in military affairs sounds revolutionary, but, in fact, it's evolutionary.

And you're going to see that there's a lot of things going on inside it. And some of the most important stuff is insanely boring. Like, how you build a ship in a shipyard is a snoozing affair.

But I got to tell you, we could save tens of billions of dollars every five-year cycle if we properly implement this. We can put it into PowerPoints, but we can put it into our RDT&E, or Research, Development, Training and Test and Evaluation cycles.

Everywhere it is, it's going to save money, it's going to save time, and it's going to give us that step up on the adversary to win, and we will win before they implode or as they implode, either one.

I want to thank three great guests here – panelists here, Leah, Ike, and Napalm, and if we give them a good round of applause.

(APPLAUSE)

MONTGOMERY: All right. We hope to see you all again soon. Thanks.

END