Disruptive Warfare: The Nonkinetic Fight

This transcript is made possible through the sponsorship of Schneider Electric

Michael Dahm:

All right, good afternoon. I'm Mike Dahm. I am the Senior Resident Fellow for Aerospace and China Studies at the Mitchell Institute for Aerospace Studies. And I'm very excited to welcome you here today to the Disruptive Warfare panel, where we're going to be talking about information warfare and the non-kinetic fight.

We're joined today by two leaders who are in the thick of those issues, Air Force Lt. Gen. Kennedy, and Space Force Lt. Gen. Schiess.

Briefly, Lt. Gen. Kennedy wears three hats as Commander of 16th Air Force, Commander of Air Force's Cyber, and Commander of the Air Force component of the Joint Force Headquarters Cyber. He's a B1 command pilot, but has been leading the way on cyber information warfare and C4ISR in the Air Force since 2015.

Lt. Gen. Douglas Schiess is the Commander of U.S. Space Force's Space, and is dual hatted as Space Command's combined joint force space component commander. Lt. Gen. Schiess started his career as an ICBM crewman, but then quickly transitioned to space launch responsibilities, and has worked in space operations since 1997, transitioning to the U.S. Space Force in 2022.

So just so we can level set the audience, I'd like to give both of you an opportunity to tell us a little bit about your commands, and General Kennedy, we'll start with you.

Lt. Gen. Kevin P. Kennedy:

All right, thanks, Mike. And if you want to fill a room talking about your command, I highly suggest you have the Chief of the United States Air Force talk about your command the day before, and then you get about 2000 people.

So a little bit about 16th Air Force. So as Mike mentioned, we wear three official hats and delegates. There's another capability that sits with us, another hat and role, is the Service Cryptologic Component Commander, which is an integration with the IC, with DIRNSA as the Director of National Security Agency.

So in our NAF, we have 10 wings in a center, with the ISR Enterprise, a portion of the United States Air Force, EW Enterprise, the entirety of the enterprise level cyber, doesn't count the base level enterprise that connects us and our Airmen to the domain, as well as a large preponderance of the information operations specialists, those that we have chained in the United States Air Force to do information operations. About 25% of the individuals, the Airmen that we train, live in 16th Air Force. And we accomplish those missions.

What do we do across that? We have forces that go from the North Pole, Alaska, all the way down to care sensors down in the South Pole region. We have groups on the peninsula in Korea. We have a group that's out in Germany.

And one of the key aspects of that is supporting CFACCs, supporting the joint force, supporting the intelligence community, and helping generate insights so we can compete now and prepare for crisis and conflict across all of our wings and centers.

The key aspect that we talked about, just to inform, I know we're not taking questions in here, but as the Chief talked about the elevation of AF Cyber is to make sure we have our alignment to cyber command

is a hundred percent clear, and the integration at the highest levels of the Air Force. And the second part is a wake-up to the DAF, is what the Chief said yesterday. And so I think we understand the importance of the domain of operating in, through and from cyber domain, as it's relating to information, turning the data into information, into insights, into actionable things that we can accomplish so we can compete, and when should we go into conflict with our pacing threats and challenges.

So that's what we do in 16th Air Force as we're going forward. What is going to be in that command? Details to follow, as we look forward and understand. Because the other key thing that we have to look at there is with Air Combat Command, and thinking, how do we solve some of the challenges you saw on the screen there? How do we make sure that we're linking the intelligence community, we're linking all parts of our Air Force into that long-range kill chain? How are we driving that readiness? How are we enabling these ATFs that are going to be at these task forces, these unit level actions at the wing level, to enable them, and connections into these larger enterprises which is successful for them to train and be ready? And also, how can they episodically, if they're disconnected at the edge, get connections enough and understand enough at the edge to be able to execute their mission?

So we're going to work through that as we follow on. But just know that the emphasis on the cyber and the information domain in the Air Force is not changing. It's there. The structure may change, but the emphasis isn't going to change.

Michael Dahm:

All right, thanks. General Schiess.

Lt. Gen. Douglas A. Schiess:

Hey, Mike, thanks for having us and thanks to AFA for putting this on and to the Mitchell Institute. I noticed our clock hasn't started, so I think that means we can talk forever, but we'll see what General Allvin and Undersecretary Jones think about that.

But hey, thanks for allowing us to be here. I am the Commander of U.S. Space Force's Space, one of the newest component field commands of the Space Force. And when we stood up the Space Force and Space Command at relatively the same time, we had a bunch of different disparate commands. And General Saltzman came in and said, "Hey, we really need to put one component that is the component to U.S. Space Command to do the majority of the mission that also allows Space Operations Command to do that organized train and equip, and force present under Space Force generation to this command, and my other compatriots in the other component field commands."

So we officially stood up on 6th December. Now, we took a bunch of commands that were already together and so we've been working together since, actually in June, when we exercised this organizational construct in PAC Space Century with Indo-PACOM and U.S. Space Command. So I'm happy to represent the Guardians and the Soldiers, Sailors, Airmen and Marines that do this space mission for General Whiting as the Commander of U.S. Space Command.

A little bit about what we do. So we have two combat deltas that do command and control for the protect, defend and deliver mission. And I'll talk a little bit more about that. So in the protect, that is our responsibility to protect the joint war fighter from space enabled threats and attack against them. So that means we have to take away or negate the adversary's use of space to target our own forces, whether that's aircraft carriers, whether that's big wing aircraft, or any of those things.

We also have to defend our own assets. We have to make sure that our adversaries can't get after our assets, because our third line of effort is we have to deliver those space capabilities that the joint war

fighter has counted on forever. As a matter of fact, I've heard general Saltzman say the joint force is size because of what space can bring to it. So we can't allow that to be taken away.

And so we have these two combat deltas that become the National Space Defense Center, and the Combined Space Operations Center that do that. And then we take the force presented, as you heard, our unit of action from the CSO earlier today, is our combat squadrons and combat attachments. We take them in their execution phase and we use them to do the mission of U.S. Space Command. We also work with the other component field commands, space forces, Indo-Pacific Space Forces Central and Space Forces Europe-Africa, to make sure that we can also provide those geographic combating commanders the effects that we need.

And then I'm glad to sit on the stage with General Kennedy. We are both components, his direct support to U.S. Space Command and we work together on a regular basis to make sure that we can do that non-kinetic fight and work together. So thanks again, and happy to be here.

Michael Dahm:

All right, great. Well, the generals have already advised me that I have far too many questions. So we'll just start through this and see how far we get in the next 32 minutes or so.

So starting with this idea about what is information warfare, the Department of Defense does not have an established definition for information warfare. They prefer instead to talk about operations in the information environment. But when you read that doctrine, the information in the information environment seems to be everything. And if it's everything, isn't it kind of nothing? It's operations in the information environment including malign influence on social media, strategic communications, but it can also drill down to the tactical level, to jamming a radar, or jamming a communication satellite. So I'd like to ask General Kennedy, how should we understand what DOD calls the information in environment? Is it really just one gigantic environment? And maybe you talk about how 16th Air Force defines information warfare in your command, and how they pursue the information warfare fight.

Lt. Gen. Kevin P. Kennedy:

Okay. All right. Thanks, Mike. So the way I think about the information environment, you can't draw a box around and say it's this and it's not that. So it's interactive from the highest levels, when you're talking social media, that's part of the information environment, is that necessarily where we focus, not in the abstract. And so where I think it's valuable for us is the United States Air Force and the Department of the Air Force is to focus on the operational level and the tactical level of military operations and how we leverage the environment. And so when the environment means is where do our adversaries' forces exist, and what information do they use. From the personnel, as well as the systems that make up that environment. So what information and data do they use, and then how do we exploit that to generate an effect that is then supported and layered with other domains.

When we talk about information, there's warfare, there's cyber warfare, there's air warfare, there's information warfare, but in general it's warfare, which is the alignment of military capabilities and to pursue national objectives, is generally how I think about that. And so in the information environment it's like, okay, what is existing in the information, how we can influence that information in the humans they're using, and the systems they're using, and the way that is beneficial to us. How do we protect our information that our soldier, sailors, Airmen, marines and Guardians are using, and the systems that they're using in a way that we have confidence in that information to generate ideas and to generate actions. So we have that effect on us.

Where information warfare in the side of 16th Air Force is we're really looking on what's the effect that we're trying to generate in the environment. And the ultimate perception and competition where we're

focused and we have a concept that we've rolled out called the Information Warfare Operation Center, which is a synergy across the CFACCs, and we've been working that in the last year, and just this quarter, just in January we had our first kind of general officer level sync with F South, with members of Global Strike Command, as well as with Nora Northcom. And those components season and brought them in and said, "Okay, the Air Force, how do we do these types of activities? And then are we producing the perception in the mind of the adversary that we want?" That takes pre-work, because the biggest question that I'll get from General Allvin or others would be, how do we know we're being effective? And this isn't a PEW research study, it's like, "Okay, what do we perceive of U.S. capabilities?" It's really about the military forces that we think we will have to face, as well as the senior decision-makers.

And the key there is, have we identified the priority information intelligence requirements? Have we identified our commander's intelligence requirements? So we have those types of observations in play and process ahead of time, so that we can get those insights as we're looking forward and we're executing that. And we're creating that perception, because in competition it's generally we're focused on integrated deterrence, and that is an informational outcome. It is creating a perception in our potential adversaries where they choose not to come in code of conflict, or crisis, and try and to negate the objectives, national interests of the United States or our partners and allies.

Michael Dahm:

All right. So General Schiess, it strikes me that a lot of the capabilities that General Kennedy was talking about, electronic warfare, ISR, battlespace environments information, there's a lot of overlap with what you're collecting from space, what's moving through space. So how do you see information warfare in the non-kinetic fight, and what kind of capabilities do your deltas bring to that?

Lt. Gen. Douglas A. Schiess:

Yeah, Mike, thanks for that question. Obviously, speaking to the crowd here, they know exactly what I'm going to say on that, we can't do space without cyber and without data and without information. So we have ground systems, we have satellites, and we have user equipment, and all of that has ones and zeros, data and information in there. And so as general Kenny was talking about, we have to make sure that we can say that we secure that area, that we know that when we send a signal to a satellite, it is actually going to that satellite, it is doing exactly what it is. So we have to look at it from a defensive cyber operations' perspective, and that's really where the space force is at now. And so do I have systems on our networks to be able to say, "Hey, this is valid, what we're actually doing is happening," and that we have the ability to see that we have done that.

And so we have to be able to protect that data. However, there's other adversaries out there that want to get into that kill chain, that want to get into that. And so then we have to have the ability to negate their ability to do that. And so how do we do that? We have counter communication systems, where we can go out and jam signals of other entities, and we can do that very effectively.

We also have to know when our signals are being jammed. So we have bounty hunter systems, different systems out there to then help us be able to geolocate where that is, and then maybe provide that to another component, or another CFACC, or CFMCC, or somebody, to go after that asset to take away that ability to do that. And so it really comes down to securing our own cyberspace to be able to do the information that we need, being able to attribute that somebody else has done something to us, and that when we're actually taking our actions, we know that what we are doing is exactly what we need to do. And General Kennedy and I have to work together to make sure that we can do that for the Space Force, for U.S. Space Command and the other components, the other geographic commanding commanders.

Michael Dahm:

So tell me, I mean, it seems like there's so much overlap: electronic warfare, cyber, all of these things that you've both talked about now. So tell me a little bit about how the coordination happens. Are you embedding Guardians and Airmen in the same task forces to achieve these effects, either through space, or through an airborne layer?

Lt. Gen. Douglas A. Schiess:

Yeah, great question. So we have some Guardians that we've put with 16th Air Force to understand their mission and to be liaison, but to really get to know their mission so that then they can come back and help us with our mission. And so I think one of the smartest things we did with the Department of the Air Force having the two services because we were so linked to keep it that way so that we can do those things. Not that we don't also do that with the other service components, but that's one area we do it. And then I think we mentioned General Kennedy and his role at cyber as a direct support to U.S. Space Command, and then I'm a component. And then in my role, General Whiting has given me, much like a CFACC has for a geographic command commander, has given me the CGIC responsibilities to work across the other space command components that also have different capabilities in the electromagnetic spectrum.

And so having to do that together, and then working with General Kennedy's folks to make sure, one, we are securing our assets, but also what can we do to make me make... I talked about us having the ability to know when we make a decision, when we do an action, we know that it's going to happen. Well, what can we do to put the doubt in the adversary that when they do something maybe it's not going to happen. And so that's where I think we work together. And I don't know, Trap, if you have anything else you want to bring to that.

Lt. Gen. Kevin P. Kennedy:

Yeah, thanks, Doug. And so Mike, what I'd also offer is, there's two kind of parallel tracks here. There's an OT&E responsibility, so we're ready to do it. And then there's an employment through combatant commands. And they're both kind of the fundamental principle like we just talked about yesterday in the main bauldrum, is there's an integration aspect that has to happen across all of that. So first we'll talk about the unity of effort type of activity where we're thinking, okay, across the combatant commands, we'll each get different authorities and we're thinking about how can we use unity of effort across space command stratcom, who we're also supporting as in general support and cyber command. So we're moving toward the same objective. And then it moves towards unity of command in general for timing and tempo of the operation. And so when the timing and tempo that's usually owned by the geographic, General Whining and space command could be the geographic, depending on where the effect's going to be.

But largely, where our planning is right now, it would be potentially, let's say Indo-PACOM, would be the one that would own that timing and tempo. But we have a unity of effort approach that then clarifies the unity of command when we have to execute the operation and create those effects.

And the OT&E side, we need to build that structure so our Airmen and Guardians understand how they operate across the domain. And as Doug mentioned, we have Guardians inside of our headquarters and we started conversations with the S3 to say, okay, how do we integrate some of the Guardians onto our joint force headquarters cyber side as well? To think through, okay, how do they understand that? So as we are growing that capability and understanding on the defensive side, which I think we're really integrated in, and the offensive side, and I think that's a place where we'll grow in the future.

And then on the defensive side, it's really integrated is talking about mission assurance and generating combat power. And the leveraging of the domain to generate combat power, 16th Air Force in our app cyber role at the execution of the Department of Defense Information Network is a joint activity. We are the components for the Air Force. We represent the Air Force in that, the Department of the Air Force. And so we'll work with whatever unit level organizations exist, cybersecurity service providers inside to make sure that that environment is the most secure and the most reliable, and the most confidence in that system across the Space Force and the Air Force. But we have to do that in competition. So when we move into times when the adversary is actively trying to come at us, and deny that type of confidence in our systems, that we have enough resilience built in, and training with our Airmen and Guardians to be able to respond.

Michael Dahm:

Excellent. All right. So turning to some discussion about adversary threats. So in 2015, the People's Liberation Army created something called the Strategic Support Force. Some of you might heard of that. For those who haven't, the Strategic Support Force is a military service level organization that in China incorporates a lot of the same information warfare capabilities that we're talking about here with 16th Air Force and S4S. So we're talking cyber, electronic warfare, space communications and the like.

The Strategic Support Force has done a lot to focus China's efforts on information warfare, space and counter space. And I could describe those, but it ranges from everything from the space plane, to counter space activities including electronic jamming, to dedicated psychological operations at something called the Three Eleven Base, which is focused on strategic messaging and media operations in Taiwan. And of course, this is to say nothing about something you're all familiar with, which is China's cyber intrusions into U.S. government systems.

So the question really for both of you is, what are the Chinese military capabilities that concern you the most? What keeps you up at night? And more importantly, can you speak to how your organizations are addressing these emerging threats? And we'll start with General Kennedy.

Lt. Gen. Kevin P. Kennedy:

Okay. Well I'll talk to, the first, the idea of what are the three aspects in the PRC that I see that we have to address inside our force. So the first one is disinformation. The capability that the PRC is using to spread disinformation, or to continue to push misinformation through the environment to achieve their objectives. And so as you mentioned, Mike, they look at information eyes warfare, which is an activity that's, this isn't a 2028, this isn't a 2035, this is a 2024 activity. This is happening today, and it's happening with us as participants into this activity. And what does that mean? It's shaping our perceptions and our behavior through the information environment about the common discourse that we have in our professional and private lives. This is the social media space.

And folks talk about, I'm not concerned about TikTok as a thing to look at videos and cats, but what I am worried about TikTok, in this sense. So I'm not really worried about the data that they take from that. It's the information in the way the algorithms can push specific things to each of us, and at position quantity to shape our perceptions, and that type of disinformation and misinformation. That's really, if we're opening, we're allowing ourselves to be influenced by the PRC. So that's the first one.

What are we doing by that? I think our responsibility in the Department of the Air Force is to train ourselves and our families in how to consume information, and do that perception management of ourselves. And so there's a couple of TTPs that I have for that. The first one is if your first response to something that you're seeing in the information is an emotional one, then you're being manipulated. Now, movies manipulate us. But just realize the information you're having, if the first one is an

emotional response, then you need to work through the logic base and understand what you're doing. And how do we do that? We teach critical thinking and problem-solving. And we have that embedded in all of our training as we're going forward to kind of understand, "Okay, what is the activity that's being happened here? What's really the activity that I'm participating in knowingly or unknowingly?" So that's the first one, is disinformation.

The second one you mentioned is Volt Typhoon type of activity. So everyone can go look on 7th February CISA pushed out a report that talked about Volt Typhoon and their intentions to preposition on, or evidence of pre-positioning on critical infrastructure. Energy sector, telecom, water treatment plants. There is no military utility that is for espionage by being on any of these networks. This is pure pre-positioning. Now, is it pre-positioning to impact our ability to generate combat power? Probably. Is it pre-positioning to maybe sow a perception in the public? Absolutely. And that's how I see that type, that concerns me the most, is as we go into a crisis and these kinds of things below the level of armed conflict, below the level of kind of kinetic operations, trying to influence our population and our responses and our adversaries.

And then the other aspect is trying to influence our ability to generate combat power out of the United States. Will it completely shut us off? No, our resilience will respond, but it will cause friction in our ability if we let, if the PRC is unabated inside of our critical infrastructure that we rely upon in the United States to produce.

And the last one is scale. So PRC has a scale, you talked about the fifth CISA, that's a pretty large organization, and they have some significant scale. How do we combat scale? We combat scale by partners and allies. Partners includes industry, it includes U.S. industry, cybersecurity, telecoms. It includes a partnership and information sharing across that enterprise so we understand the adversary and the threat, so we can build our resilience and build that posture. So if the adversary tries to disrupt us, we're ready.

Michael Dahm:

All right. General Schiess, what keeps you up at night?

Lt. Gen. Douglas A. Schiess:

I sleep pretty good, mostly because of the Guardians that are out there doing the mission today. And I know that they've got it in hand. But to talk about China specifically, and I will get to the information part of that, but just as I said in an earlier panel today, I mean, China has the ability to touch our satellites with a direct descent anti-satellite missile that can take our ability to communication, missile warning, ISR out right away. So they have that. They have demonstrated taking another satellite and moving it to a different orbit. And they've talked about how that could be done to get rid of debris. Well, it also could get done to get rid of one of our satellites. And so those are all kinds of things, but the information spectrum, they can jam us all the day. They have so many jammers, it's just incredible there.

So we have to find out how do we be resilient, as general Kennedy talked about, with our communication systems, because we do need data to do our joint war fighting, and we need to do that. So how do we fight through that? And then obviously, their cyber capabilities. This is not China, it's Russia, but at the beginning of the Ukrainian invasion, Russia actually hacked into a commercial satellite system that they thought would be constrained to that area, but actually affected a lot of users in Europe. And so we have to be prepared that China can do that as well. And so those are the things that I talked about.

But to get to how we're getting after this, one is that defensive cyber operations that I talked about, the ability for our Guardians to know that their systems are protected, and that their systems are actually secure and doing what they need to do.

And it makes me think about 24, 25 years ago, when Captain Schiess was operating the GPS satellite system, if something happened to one of those satellites, I did not think that somebody was messing with one of my satellites. I thought, "Oh, there must be a bit flip. There must be something that happened. Let me restart that." That is not how our Guardians think today. As soon as something happens on one of their systems they're looking at, I get the reports, the commander's reports, and it'll come back and say, "Well, we've looked through, we've talked to 16th Air Force, we've talked to others, and we know it's not this." And so they are thinking, because they know that they have an adversary out there that's going after. And so we just have to continue to develop our Guardians as the CSO talked about, so that they understand the cyber environment so that they can be the best war fighters they need to be.

Michael Dahm:

All right. Yeah, I spent a little time at sea when I was in the Navy, and I asked those same questions. "How do you know our satellite communications aren't being jammed, chief?" And he's like, "Well, I don't know, but we usually just turn it on, and turn it off, and turn it back on again, and it works."

Lt. Gen. Douglas A. Schiess:

That's what Chief Coffin says too. But he's learning too. And we have to get away from that, and get into, how do we get around that? We talked about PAC Sentry with Indo-PACOM, and General Mastalir, and I talked about what are the most critical links that are out there, let's maybe move those to different communication satellites now, let's cause confusion in them on where they're going after the most important satellites working with our commercial partners. And so we have to think a lot harder than Captain Schiess had to think.

Michael Dahm:

So sticking with this threat theme, General Kennedy, you talked about perception, and about educating people about the threat, and understanding how our perceptions might be shaped. So I look at a lot of Chinese television, a lot of Chinese news articles, and the People's Liberation Army has a very well-curated image. They are putting images out on the internet, and TikTok videos on the Chinese internet. They look awesome, they look 10 feet tall. They are the force to be reckoned with.

And so I understand when our leaders go to Washington, they have to get above the noise floor, that persistent noise floor in Washington DC to bring attention to the fact that our Air Force and our Space Force need resources to do our jobs. But the question really for both of you is, how do we reassure our allies and partners? And how do we actively shape the PLAs own perception of their limits to their own military capabilities? How do we publicly argue for resources with our leadership? Because in some areas we are losing ground, but we don't want to play into the Chinese game of making them out to be 10 feet tall.

Lt. Gen. Kevin P. Kennedy:

Thanks Mike. So I think that's a balance. First, we are the greatest air and space force the world has ever seen. Period. Now, we want to make sure we stay there. And as we look through the organizational construct and re-optimization, that's one of the things we're doing. And as the secretary talked the OI series, that's capabilities, let's make sure we're looking over the horizon, and looking at the threats

being clear-eyed about the threats that's coming. With written our force is the information, again, you're talking about an informational outcome here. This is about integrated deterrence, and creating the perception in the adversary of understanding the reality that should they challenge the air and space force, we will fight and they will lose.

Now, we don't want to win by a goal, or a run, or pick your sports metaphor. We want to win by the first half, or preferably before the game starts, right?

Michael Dahm:

Not in overtime.

Lt. Gen. Kevin P. Kennedy:

Not in overtime. Although not a bad game. But that's really where when we're talking about deterrence, it's like they should not choose to challenge the United States. And when you add our partners and allies, which that is the biggest strategic advantage I think the United States has prepared to potential conflict in the Indo-Pacific region, is that we have partners and allies, and generally our adversary has clients. As we continue on that, I think that is where we go. But we have to be clear-eyed about the threat. And we have to make sure that our senior policy makers understand, this is the threat, this is where we see them going, and we reveal and expose those types of activities. We reveal our capabilities to deter them. We shield, and we do not expose some of our capabilities because those are necessarily to defeat. They exist. We keep them held closely, because we need to make sure that they're there when we reach for them.

And then we will disrupt their attempts to meet those perceptions and change those things. And those are things that we will do every day in competition, and then we'll be able to move through crisis and conflict. And a lot of what we think in 16th Air Force, what we do today is generally in scope of what we're going to do in crisis or conflict. What's going to change is scale and intensity. And we talk about scale, again, scale is partners, and scale is enterprise. That's how we do that. And intensity is training and readiness. That's how we get ready for that.

Michael Dahm:

So, over to you. I mean, so many space force capabilities we cannot talk about, but we're trying to shape perceptions.

Lt. Gen. Douglas A. Schiess:

Right. Yeah. It gets into the reveal and conceal and how do we keep the things that we need to at the classified level. But I will say it, I think General Saltzman talked about this morning with under the Deputy Secretary of Defense and our new security policy. We're going to get after how we do the right classification levels for the things that we need to protect, but also being able to talk to our allies. So under U.S. Space Command, there's a named Operational Olympic Defender, and General Whitening has given me the operational commander for that. And what that means is, with the UK, Australia and Canada, they are right there with us. Those individuals are sitting on our ops floors with us. I have regular conversations with their commanders of their space command, and we are getting after being able to provide information to them at the classified level, and also making sure that we are talking with each other so that we all know what each other is doing. Because we have to do this together.

Our allies, if you take an action in space, it doesn't just affect the United States, it affects the world. And so we have to be able to talk to our allies. We're going to continue to add allies to that. But to your point about, how do we communicate this, I think one, we are communicating more to the American public

about the need for the Space Force, and having 30 years in the Air Force before I transferred the Space Force, General Kennedy had it right, we are the best air and space forces in the world. But it is the time, and we get to as the CSO said, reoptimize for great power competition.

And so that's what we're getting after in the Space Force, and in my job at U.S. Space Command, to make sure that we don't let the Chinese, or the Russians, or whoever, get to where we're winning in overtime, we're winning before the game even starts. And so we have to continue to communicate that, we have to continue to work with our congressional leaders to get the funding that we need to do, because we need to be able to have these capabilities on orbit to be able to protect the joint war fighter.

Michael Dahm:

All right. I think we've got time for one last question. So, the global war on terrorism was a very different kind of fight. But it largely took place in a benign electromagnetic environment. If you were flying over Afghanistan or Iraq, you didn't really have to worry about your GPS not working, your calm not working, your radar not working. But I've been looking at the PLA for almost 20 years now, and this is one area where I think the PLA may actually be eight feet tall, maybe 10 feet tall, but they put a lot of effort into their electronic warfare capabilities. And so I'll just read a couple of things here.

The Air Force rewrote Air Force Doctrine publication on electromagnetic spectrum operations, and I'll read from it. It says, "The joint force requires an over matching offensive approach to electromagnetic spectrum operations to enhance competitive advantage and create multiple dilemmas for adversaries in all domains. General Allvin, when he was vice chief, he was quoted, 'In order to align with national defense strategies, the Air Force will need to embrace new concepts for electronic warfare and increased emphasis on the broader electromagnetic spectrum.'" So how would you rate our electromagnetic spectrum operations capabilities with your own organizations and across the joint force, and how do you think we can take our game up in this critical mission area? General Schiess?

Lt. Gen. Douglas A. Schiess:

Yeah. Thanks, Mike. Obviously, this is an area that we have to continue to get better at. And so you talked about the global war on terr, and I was actually deployed as the director of space forces to CENTCOM during that time, and there was GPS jamming during that time, and we actually dropped some JDAMs on some GPS jammers. And so we have to have the capability to know where that jammer is. So we have to have the ability to geolocate, we have to work with our intelligence community, we have to work with 16th Air Force and others to be able to know that spectrum. We also have to ensure that the joint war fighters, including ourselves and other services, have PACE plans, they have the ability to go to different communications systems if they need to. I think we have seen in the Russian aggression what a proliferated low-earth orbit can do for you to be able to have data get to who it needs to at the right time. And so we have to go after capabilities to do that.

And so that one jammer is not enough, now maybe that could cause some issues later, but it also can continue to keep the data flowing. And so we have to continue to get better at that. We have to train our Guardians to be able to look at things and go, "Hey, that's not right. There's something going on here I'm going to investigate. It's not an on off kind of thing, but we have to be better at that." But I know that our Guardians are doing it right now, they're doing it today, finding signals that are out there, going after providing that information to combatant commanders, and then helping the joint war fighters use the electric man spectrum that they need to. And so we will continue to get better at that, but it's something that we can't just rest on our laurels. We got to continue to work on it.

Lt. Gen. Kevin P. Kennedy:

Right. And to piggyback on what General Schiess said, is the Airmen and Guardians out there today understanding the baseline of electromagnetic spectrum. And that's pretty critical. As we move into crisis and conflict, we got to understand what the natural baseline looks like, so we can have that freedom of action when we need to do it, and we need to make sure we can use the electromagnetic spectrum in the ways when we have to execute our operations. Having superiority over the whole spectrum, I don't think that's possible, but having it when we need it, is necessary. And so that's one thing we have to think about there from a defensive aspect on that.

The other one is we're looking forward is really building in resilience, like Doug mentioned. How are our systems building in the resilience so they can operate through what we know will be a contested environment in the electromagnetic spectrum. On the offensive side, I think if you want to talk where we are, I think there's great promise, and we're seeing good integration on that. We're looking at the integration of all of the capabilities with the cyber capabilities that we would have, our ISR folks helping characterize the environment and understanding what apertures are available, and then really aligning those. And that's from space, all the way down to the sea.

Michael Dahm:

All right, great. So we're under our last few minutes. I still have several questions, but we will not get to those, regrettably. But I would like to thank our panelists for coming today. And General Schiess, I'm going to give you a couple of minutes to wrap up. Any closing thoughts from you?

Lt. Gen. Douglas A. Schiess:

Hey, thanks, Mike. Appreciate you doing this. Appreciate AFA for this forum. And I appreciate everybody here coming to listen to this, and I thank you for what you do each and every day for our nation. The time is now, as secretary said, we're out of time, and so we have to reoptimize our services to be able to get after the great power competition of China and the other adversaries out there. And so I thank you for what you do. I'll tell you right now, I'm amazed at what Guardians and what Airmen can do on a daily basis, and I know that you're going to continue to get after it, and we're going to get out of your way, and we're going to point you in the right direction and help you get to where we can be the best air and space forces, continue to be the best air and space forces for the world.

Lt. Gen. Kevin P. Kennedy:

All right, roger that. And first I want to really thanks for the partnership with AFA and with the Space Force as we go forward on that. And to take the Chief's words, what we need to do now is as we continue to move forward, its follow through on our understanding of the domains and where it needs to go, and continue to follow through as we do this optimization and redesign, to make sure that we're capturing the value in the enterprises so we can compete and win in the electromagnetic spectrum, the cyber domain, ISR, you name the enterprise, we need to go forward and do that. How do we do that? For me it comes down to three things.

First, is we look at our allies and partners. External to the United States, in the interagency, within our department, within our service, that we have to make sure that we are maximizing that value. And with industry. We're at an inflection point that these are critical times and periods like the Chief talked about, where we got through this previously with a really tight partnership on technology and innovation, and with industry, and how we move forward. We need that same thing in this phase, in this time of our nation.

The next thing that we need is resilience. Resilience of our Airmen and Guardians, resilience of our systems. If we go in thinking we're going to have exactly what we have now during a conflict, we are going to not succeed. We need to understand that and then build in that resilience in the system.

And finally, the people that understand what data they need, the side that understands that, translates that to information, and gets it to the point of maximum military utility is a side that's going to win. So thank you, and I'm really excited, every time I see a room full of Airmen and Guardians that come to hear about information warfare.

Michael Dahm:

All right. Well, that brings an end to this discussion, but I can tell you that I have been a student of information warfare for a long time now, and I've become thoroughly convinced that the future fight, the future near peer fight, is going to be decided within the C4 ISR system of systems that these two gentlemen are responsible for. So please, join me in thanking them for their time, and have a great air and space forces kind of day.

This transcript is made possible through the sponsorship of Schneider Electric

Schneider Electric™