Space Domain Awareness

This transcript is made possible through the sponsorship of Schneider Electric

Maj. Gen. Gregory J. Gagnon:

Hey, good morning. Happy Valentine's Day to everyone. You're already losing because you're probably away from home. That's all I'm saying. Secretary Jones, thanks for joining us this morning and to all the Guardians and Airmen who took the time out this morning to choose this panel, we say thank you. We're going to talk about space domain awareness. If we could bring up the slide, that'd be helpful. These are a set of documents that are inside the Department of Defense. They've all been updated or they're brand new. Today, we're talking about space domain awareness, the ability to do surveillance and reconnaissance of space for space, to inform the seven joint functions, right, the seven joint functions. We need to inform maneuver, protection, fires.

We need to inform information for commanders that might be friendly force information requirements, and we need to satisfy priority intelligence requirements of those commanders as well. Yesterday and the day prior, we had panels on space order of battle. Notice we didn't call it catalog. The language is different. The purpose is different, which is why you have a United States Space Force, because if our sole function was combat support, we'd be a combat support agency. We're not. We're a military service. I am very grateful for our industry partners that have chosen to join us here on stage. I'm going to do a short introduction of each one.

Then, they'll talk about their main business lines. Then, we've crafted some questions that we'll work through in the next 37 minutes. First on stage, we have both old and large, and new and small, and we start with new and small, and we start with Bryon down the end. Bryon used to be in uniform as an Airman. He's a cyber security specialist. He's also highly involved in Kessel Run. He was one of the original starters of Kessel Run in the Air Force. Now, because he had all that great Airmanship and training, he started his own company and that's called Rise8. He'll be our key speaker this morning that not just talks about how you orchestrate your data, how you curate your data, and how you use your data, but for all of our defense industrial base here, how you protect your data.

Because the only thing that makes me sad on Valentine's Day is when your intellectual property helps inform the space systems division of the PLA. They are coming for your data. In fact, they have taken some of your data. You may have heard about that on the previous panel. Next, Pablo. Pablo comes from one of our primes and he represents Northrop Grumman. He's been there a while. He's done a number of different things with Northrop Grumman, who is a key partner of the United States Space Force and the Department of Defense in all parts of space, both ground, both in the orbit and in the link. Then, finally, the good doctor, Dr. Parker is from Boeing. She's been with Boeing for some time.

Many, many, many of the satellites we operate in space today have her fingerprints on them, either from the factory, or from the project, or from the final delivery. Ma'am, pleasure to have you here this morning. If I could, let's start with Bryon, just give us a little bit of overview of what your daily portfolio looks like. We'll work down and then we'll start the questions.

Bryon Kroger:

Thank you. Yeah. At Rise8 we do custom software development for critical missions and we help war fighters achieve continuous delivery. If you're familiar, there's a State of DevOps report that comes out every single year and it benchmarks organizations from a software delivery performance perspective. There are four categories, one of which is elite. We often say that we provide elite software development. What does that really mean? It means that we get to the point where from a software

delivery performance, we can ship software to operations, even on secret and top secret networks, daily. Our lead times are measured in hours, that our mean time to restore and change fail rates are the lowest among the industry.

That we have high reliability and security performance. Those benchmarks, we've been able to achieve them in the Department of Defense, several organizations now, without sacrificing the quality or even the RMF process that everybody loathes these days. But then for our customers, that can go a little bit farther in their journey. We help them not just build software, but build software delivery organizations. Software factory has become a bit of a nebulous and ill-defined term, so I just say software delivery organizations. The software we build today will not survive first contact with the enemy. It's more important that we build organizations that can sense and respond to the battlefield with software, software delivery organizations inside of our force.

We help them do that and we've got a very large space in Air Force portfolio as well as Department of Veterans Affairs, which is now near and dear to my heart, and will be to a lot of you someday. Thank you.

Pablo Pezzimenti:

Well, good morning. Thanks for the opportunity. I think my three teenagers will agree that I can be described as old and large. All kidding aside, appreciate the opportunity. Thanks very much. As you noted in the introduction, I support the organization within Northrop Grumman that houses the bulk of the ground scope for our space sector. That's a pretty broad portfolio, lots to talk about there. A very large and important part of that is our ground-based space domain awareness work. We'll get a chance to dive into that as we get into the Q&A, but just really want to thank you for using the forum to highlight space domain awareness as so important, not only to what happens in space, but as you noted to what happens across all the other missions.

As I think through all the missions that I've been a part of with Northrop Grumman, many of them space related, many of them not space related. It's very difficult to think of any that don't have a dependency on space to be successful. Topic at hand, very important, appreciate the opportunity.

Dr. Michelle Parker:

Okay, good morning. Thank you. I want to thank AFA and General Gagnon for hosting this panel. I think it's an important topic to talk about and ever evolving as threats evolve and the space environment gets more populated. I run the Boeing business called Space Mission Systems. That's all of our satellite work and groundwork and associated groundwork. Although I will take the mantle of old and large, we've been building satellites since the 1960s, launched our first satellite in 1963, the first geosynchronous communication satellite. We have a long history, but I hope through this panel I can convince you that we're also small and agile and ever evolving.

Within the portfolio that I lead, we have a lot of space domain awareness activities. I would point out that it's not just space-based, it's ground-based and the networks that support all of those systems. We operate the Advanced Maui Optical Surveillance site on Maui, so it's ground-based surveillance. We also were a contractor on the space-based surveillance system, space-based. Then, we operate one of the really important networks that carries the DOD's, SDA data, and I think we'll talk a little bit more about how important networks are as well. As the domain continues to evolve and threats evolve, it's going to be important that we are able to rapidly deploy capability.

We've demonstrated that recently with our Subsidiary Millennium Victus Nox in partnership with the Space Force. Getting Victus Nox up and reconfigured in eight months and launched and in-service within a couple days. Really breaking the timelines of what we would've thought just a couple of years ago

were possible, so really a great achievement. Then, most recently we've launched the X-37 and are testing out new SDA technologies there. We've got a lot going on and we're really proud to be a part of the SDA approaches and evolving technologies.

Maj. Gen. Gregory J. Gagnon:

February 14th has started like February 14th for me in many years, where I say something and it's misconstrued. It's good to see that doesn't change what state, whether I'm in DC with my spouse or here in Colorado. Pablo, let's start with you in how space domain awareness, specifically the comprehensive ground-based and space-based SDA architectures, support competitive endurance. Competitive endurance, as you know, has three elements, if you will. One is avoiding operational surprise. The second one of course is to deny first-mover advantage, disincentivize the adversary from starting a war, if you think of it that way. Then, finally, responsible counter-space campaigning. To make sure that we can hold that risk, those military capabilities that hold our joint force at risk. Can you talk about how you're involved in that?

Pablo Pezzimenti:

Sure, absolutely. The National Space Awareness architecture has definitely evolved, as you noted, over the last few years. We used to talk about space situational awareness, right? Today, we talk about space domain awareness, and that may seem like a subtle change, but it's not. It's a pretty substantial change, particularly as it relates to the requirements for the architecture that is meant to deliver against SDA. Now, as we look back at the ground and the space-based assets that we're a part of, at the management of the data itself within the architecture and at our actual engagement with the end users, all of that has evolved.

When you talk about sensors, ground-based sensors and space-based sensors, you look back to the 1980s and some of the first electro-optical sensors that Northrop Grumman developed and deployed. Those met fully the requirements at the time. That's because if you had some cloud cover, you could literally come back a few hours later, maybe a full 24 hours later, regain custody of what you were tracking and all what's good with the world. That's far from the environment we're in today. Persistence is absolutely necessary. It's not a nice to have, it's a must-have. Those ground-based sensors have had to evolve over time and they have, and they've been supplemented with RF sensors.

The latest of which you well know, Sir, is the dark program that the Space Force had teamed with Northrop Grumman to deliver a couple of years ago now. That's going to be a real game changer in terms of our ability to have persistence at the full GEO belt, the ability to know exactly what's going on at the GEO belt. Beyond the ground-based sensors, there was also the addition of space-based sensors not that long ago. I guess it depends what your time range is, but certainly space-based sensors have now also supplemented some of the gaps that existed on the ground and really expanded the mission to also include some of the things that you noted.

Like neighborhood watch in space, as well as critically the ability to really characterize what's going on out there. Not only knowing where things are, but what their capabilities are, for us to be able to answer the mail fully for space domain awareness beyond space situational awareness. The sensors themselves have all evolved both ground and space, and then how we manage the data has also evolved. From a very centralized approach historically, to a much more distributed approach, working as much as you can in terms of the management of the data and also the processing of the data at the edge. That's on the ground certainly, but also in space, pushing as much of the processing to space as possible.

That is important for a couple of reasons. In terms of data latency, super important, but also from a comms perspective, right? Our ability to really answer the mail and address some of the bottlenecks

really requires us to push some of that into space. Finally, and I'm sure you'll chat about this quite a bit, how we engage with the user. The operator has really changed a lot over the last few years in terms of making sure that they are part of contributing to the solution. We cannot surprise the operator with what we're pushing out. As software gets pushed out faster and faster, we have to make sure that they are ready for what's coming, that they are trained on what's coming, and that they trust what's coming.

Without that trust, regardless of how strong the architecture is, we are never going to get fully optimized the value of it. Everything from the sensors, ground, space, to the data, to the ultimate, the operator, it has all evolved to be able to answer the SDA mail. It's all foundational to our ability to really deliver against the vision that General Saltzman has laid out with us in terms of zero operational surprise in space.

Maj. Gen. Gregory J. Gagnon:

Thank you. Yup. We covered a lot of ground there. Dr. Parker, we're going to go to you next about how space domain awareness is informing how you're designing both commercial satellites and national security satellites. But before we do that, I will tease out a few things on what you said. One of the key things that Pablo talked about was having multi-phenomenology for being able to observe outer space. It's the ability to observe outer space based off the premise that you expect your adversary to move. You expect your adversary to be cunning, so you need to not just observe them, you need to have track. That is a transition basically in requirements over the last 10 years.

The second part of this that's incredibly important that he highlighted was the latency issue. I will tell you that in my office, at the classified level, I am measuring how long it takes from sensor data to UDL. I have a metric for every sensor, because data late isn't useful if things are moving around because you're two moves behind. Data latency is incredibly important. Inside our architecture, we inherited a lot of old stuff. I've been to some sites that have stuff that's my age. Okay, that's some old stuff, okay? The connectivity to those sites is one of the best investments we can make because we can speed up how quickly they can move data to the UDL.

If I was to share with business what my simplified OV-1 is, here it is. Sensor to Barb Golf's unified data library at SSC. Operators, their application is going to be agile, right? We're going to use agile software development, understand their requirement and build the tool that they need to answer their command and control or intelligence question out of the UDL. We're already doing that. We're working with Palantir and a few others, so we have a sandbox that sits over the UDL data repository and allows us to build those specialized tools. This is all set in the larger context of Atlas and other programs, but much of this is moving ahead rapidly.

The key tenets that you talked about, multi-phenomenology, sensor speed, if you will, in receiving the data and the ability to task it, are all the MOPs of this larger architecture. Doctor, could you talk to us about the things you're working and how these new requirements are changing what you are building for both commercial space and national security space?

Dr. Michelle Parker:

Yeah, thank you. Yeah, so we do do both government systems as well as commercial systems. We've historically done that, so we work closely with our commercial customers like SES, Viasat, Intelsat are all customers of ours as well. If you think about it, they're operating in the same environment. When we talk about a contested and populated space environment, the commercial operators are right there in the same environment with all of the other systems. It's critically important that we do understand what is going on in space and have the data from SDA to inform the designs of both our government systems and our commercial systems. Although we don't operate the commercial systems.

We build the systems and hand them over to our customers to operate, so they're the ones operating there, but we do work with them very closely to understand what their operations will be, what environment they'll be operating in, and how they can best approach that. I think it becomes even more important as we talk about blended architectures, where the government is going to leverage commercial providers, commercial services. It becomes even more important to understand what the threats against the commercial satellites may be. That could be whether the blended architecture includes hosted payloads on commercial providers or commercial data or communications data coming down through those providers.

Whatever form that takes, we're still going to have to understand what the threats to them are, and it could affect designs just like it affects on our government side. It could affect design decisions such as Delta-V or protected communications or orbit selection. How do we diversify the orbit? All of those things we look at both on the government side and the commercial side and really understand what our commercial customers want to be able to operate through. As we look at this as an overall integrated system and a layered system of where the different data will be coming from, it's going to be really important that we continue to have a very thorough understanding of both the existing threat and the evolving threat to make sure that we're designing for that.

Maj. Gen. Gregory J. Gagnon:

One of our commercial partners did a wonderful job about two years ago of recreating the SJ-21's capture of that defunct beta satellite. From a threat perspective, what's not commonly understood is that was a non-cooperative capture. People always say, "Oh, we have things in space that can move up to other things in space and connect." Some of our major space companies have proven that capability, but they've proven that capability with a cooperative target. We had a satellite that wasn't working, that was Chinese, that they went and grabbed and moved. That threat environment is pretty profound from a technological standpoint, which gets to why Pablo talked about having what I would call protection zones and observation zones.

Named areas of interest in space in order to protect high-value assets. You called it neighborhood watch. If I could, Bryon, you've worked software development for a long time. You've been both inside the government and now outside the government. Can you talk about any of the challenges that you have with devops, specifically with integrating and working with the UDL?

Bryon Kroger:

Yeah, absolutely. I think it's important too to zoom out and look at when we talk about data and integration, everything that was announced on day one, software powers, all of that. It's been about a little over a decade now since Andreessen famously penned that software is eating the world. A lot of military thinkers have said, "If software is eating the world, it's certainly eating the war." It should be intuitive by this point, but if it's eating the world, it's also eating its orbit. Everything that we do in space is going to be powered by software. Every ground system, every network, every single thing is powered by software. We saw this in Ukraine when Starlink was able to send over-the-air updates to block or change, and be able to be a countermeasure against Russian jamming.

These kinds of capabilities are critical. Unfortunately, our ability to deliver those in the Department of Defense is still very limited. We'll sit up on these stages and talk about all the advanced things that are coming down the line, but the dirty secret is everybody in here is still waiting for their emails to work. There's a lot, UDL gets a lot of unfair criticism in my view, as does Kessel Run and every single one of these software factories. Because in order to do what they've been tasked to do, they have to solve a whole bunch of enterprise IT problems that are not their fault, and fault and responsibility don't go

together. The successful organizations I've seen like the UDL take things that aren't their fault and make them their responsibility.

They've addressed them as best they can, but there's a lot of underlying infrastructure challenges when it comes to cloud. For instance, the first two parts of the NIST definition of cloud computing are self-service and on-demand. I've yet to run across an enterprise cloud in DoD or the Fed Civ space that is self-service. On-demand usually submit 1520 trouble tickets and wait a few months just to get access to your resources. We've integrated with UDL quite a few times, I think it's a great capability. Most of the problems I see with it are inherently limitations of the underlying infrastructure, networking, as well as cloud platform that's available to them in the ATO process. When I look at an organization like what Kessel Run did, and don't get me wrong, Kessel Run has all kinds of words.

I know better than anybody because I was responsible for a lot of them. There's a lot of things I would do differently, but what I'll tell you is the DIB once said, the number one thing that Kessel Run provided to the war fighters was hope. Very cheeky thing to say, but what was that really? If you look at it, we finally started achieving outcomes. We always have the impacts that senior leaders want to achieve, and then execution teams focus on all of the activities, so resourcing activities and features. We assume that if we meet all the features in the specification sheet that we'll achieve outcomes. But that missing gap, what humans actually do with the software you deliver them, we never check back in to see like, okay, we met the requirements back, but is it achieving the senior leader impacts?

Because of the human behaviors, the outcomes are changing in the mission space. What really changed that Kessel Run, everybody talks about all kinds of things that they did, but I think this software factory movement in general provided us two things. Number one, unlocking continuous delivery. Truly being able to deploy software on demand to operations environments without a two-year ATO process. Literally, we can start a design with a user on Monday. By Friday the design is complete and the next week it's in operations. We can do that now, that's a solved problem. What that really unlocks, that's even more important, and this is where it relates to how do we move forward with UDL and even great power competitions, is the ability to learn.

The big problem in the department, especially in the acquisitions process, is that we've optimized for being right. We spend tons of upfront time on planning and then assume that if we follow the plan, we'll get it right. But we know that's not true in the modern era. Even the best designers in the world, Amazon and Microsoft have both done studies on this and they employ the best designers in the world to design solutions for net new solutions, what we would call innovation. They get designs wrong 90% of the time, which lines up with most poeple's R&D. We know that R&D budgets, 90% will never see the light of day, and we bank on the 10% that takes us to the top. For existing systems where we're adding features to them, they get new feature requests wrong two-thirds of the time.

These are the best of people in the industry, and so continuous delivery unlocks our ability to put things into the hands of war fighter, get real feedback and learn so that we can make it right. That's the thing that we should be focused on. What's limiting us, the challenges that I see to that today is that underlying infrastructure. Every organization that sets out to deliver mission applications, even the simple ones, is looking at a scenario where there's no development environment for them, or if they get access to one, either by luck or sheer force of will from a bunch of Airman coders cobbling together a platform. Or, they're paying a large feed to the enterprise to use the solution like platform one.

If they can get through all of that, then their deployment environments are limited as well. This ability to take solutions into production is an enterprise IT challenge that we're still not addressing. I think the last thing I'll say on that that is problematic is when that starts to happen, then enterprise's natural reaction is to mandate the enterprise solutions. That's potentially the worst thing you could do in that scenario because now you've removed all incentives for the enterprise IT providers to provide a good customer

experience. If you have to win people's business, you provide a really great service. If you're mandated, all incentives go out the window.

The thing that we're trying to work with the department and all the way up at DOD and even congressional levels is to set benchmarks for DevOps for how do you measure your environment. Before you go about mandating, this is the mandated cloud solution or this is the mandated platform solution, making sure it's actually meeting customer's needs. Everybody's got their minds wrapped around efficiency, but we still haven't figured out efficacy yet. That's where I think the focus should be, is how do we get efficacy in the IT infrastructure?

Maj. Gen. Gregory J. Gagnon:

Yeah, so for my initial looking under the hood, there's a lot of infrastructure issues that are inside our space domain awareness architecture, because much of the first principles of when it was designed, it was designed really in many ways for science and technology initiatives. We have labs using things and things like that, and their timelines for making a decision are dramatically different than the timelines required of a US Space Commander, General Whiting. I highlight a few things that you talked about and the successes we've had with the UDL already. The UDL has over 4,000 users already registered that used data from the sensor suites to help make decisions. In those 4,000 users, we have 22 foreign partners.

It is a rubric that will continue to move forward. On Monday, I was on a stage at a different location, but I told everyone that one of the challenges I had seen earlier in my career was, at Air Force Space Command, was what I deemed the good idea ferry. Every time the good idea ferry came through, we changed the plan and we made no progress. The UDL is our unified data library. It's compliant with the larger DAF initiatives for JADC2, and the things that we're doing with C2BMC, and we are making progress. The key thing we have to do as senior leaders is remove obstacles and stay the course, because as we heard in the big ballroom, we're out of time, we're out of time. Thank you for that.

If I could, I'd like to pivot to the larger defense industrial base with a question about how do you internalize and do cybersecurity inside your programs to help protect your intellectual property? As they think about their responses to that, I'd like to highlight for the audience just some of the initiatives of the National Security Agency. The National Security Agency has the Cybersecurity Collaboration Center of which they're partners. We don't publish all the companies that are partners with that, but it's open and it's free. It's open to both large defense industrial primes, but also those smaller companies. Things you can get from NSA as joining their partnership is you can get protective domain name server.

You can learn which websites are malware hosted, and they give you that so that you can block that on your internal network, because often that's how malware gets into your network. People go to a site that is a foreign intelligence site, okay? The second thing they can do is they can help you understand what your attack surface looks like from the Beijing or Moscow perspective. They do that for free. The final thing they do is they provide you real time intelligence updates on what malware and what the signature looks like on different networks. Now, people would think that all of that for free would be enough to secure our IP, and it's been taken advantage of by our primes.

They understand this, but for the smaller companies in the room, you are as much a target as the primes. I beg you, help me help you keep your intellectual property for profit and don't share it with the CCP. Over to you.

Dr. Michelle Parker:

I can start on that. We take cybersecurity very, very seriously, across the whole Boeing business, commercial airplanes, defense side, everything. Extremely important to us. We have our internal

organization within our information technology group, that that is their sole purpose in life, is to protect the data that we generate within Boeing. It keys on exactly what you said, General Gagnon, understanding the threats, understanding the evolving threats to constantly be updating those protections based on the information we're getting as things evolve. It takes the whole company. There are things that come into our email that are tests like, are you going to click on this?

It is an education across the company as well to make sure that all of our employees are cognizant of the threats that are out there because they are real and they happen every day. Again, we have an organization specifically set up to work with partners and understand the threats that are coming in. We take it, of course, just as seriously on the systems that we design. Our space systems, our ground systems are designed from day one with NSA crypto or what the requirement might be to ensure that those are protected as well once we deploy them. It is a everyday threat that we are vigilant against.

Pablo Pezzimenti:

I appreciate you highlighting some of the things that are out there for free for folks to take advantage of. As a prime, if you will, we not only have to worry about what we're doing, but also a lot of the folks that we're teaming with. It's really important for you to be... We share a lot of those resources that you touched on with a lot of those subcontractors that are so critical to our ability to do what we do. Cyber and space have a lot of similarity in terms of where the first impact might come from, and we absolutely take it seriously. The training is thorough and constant and the insider threat piece of it, critically important. Sometimes much more important than the systems or much more vulnerable than the systems, I'll say.

It's an area where we focus a lot of our time as well. Absolutely an area where the primes work together to make sure that the whole ecosystem is doing what's needed to make sure that we're well-protected.

Maj. Gen. Gregory J. Gagnon:

Just on 31 January FBI Director Ray was testifying and he talked about the insidious nature of insider threat. He talked about how, very openly at an open hearing, about how the CCP will threaten families back home in order to gain leverage on employees of not just academic institutions, but also across the defense industrial base. On my nightstand, I've been reading World War II books about the history of spying and espionage. None of this is new, but we just need to realize it is real and it is present. The other thing he highlighted was Volt Typhoon, which is the new threat actor that's been identified as PRC-sponsored threat malware. That unlike the intellectual property theft that we've been talking about a lot, is initial what Cyber Com would call OPE, operational prep of the environment.

It's putting their malware in places that give them better understanding against critical infrastructures, because at the time and place of their choosing, they would like to execute critical infrastructure attacks. That's the intent behind it. That was shared by General Nakasone, who was one of the other key people there. Key to Ray's testimony was offering up how busy his counterintelligence elements are across the United States with industry. He says not a day goes by that they're not opening a new case. It's very real. Another free resource from the federal government is to engage your FBI office when you think you have an issue, and the FBI, they're there to help.

Dr. Michelle Parker:

I think those latent malware, that concerns me more than anything. If you could hit, you know it. If there's something residing in there waiting for a later time, it's very problematic.

Maj. Gen. Gregory J. Gagnon:

One of the things we've done in the Space Force is understand our cybersurface, if you will. One of the things that is most secure is the stuff that we're putting on orbit because we're thinking about it all the time. The second part of that is the installation and the critical power, cooling, fuels, and things that are on installation. Then, the third thing is outside the gate. If you're outside Buckley or you're outside of federal areas, what does the electric company know and what are they doing? For the federal government, the agency that works with that is the Department of Homeland Security. They also work through CISA, which is an organization run by Jen Easterly.

There are services available for them. What I would ask you is, are you aware, because you have major factory and production centers, are you aware of your critical dependency on commercial infrastructure that's not owned by you? Is that part of your analysis?

Dr. Michelle Parker:

That is definitely part of the threat analysis and understanding what those impacts would be. I think if we could talk about electric, we can talk about networks. None of this works without networks, electricity, water, and so yeah, we're very aware of that and take that very seriously through our security and protection organization that looks at those threats and keeps our sites safe every single day, and works with the local authorities as well to understand that.

Pablo Pezzimenti:

Yeah, and all of those things are often taken into account when we're talking about redundancy and ensuring that we've got multiple locations to do similar things. Ensuring that they're not all tied into the same hub that would be impacted in that way. Absolutely, it's always something that we take very seriously and bake into the equation.

Maj. Gen. Gregory J. Gagnon:

As a parting shot from each one of you, if you don't mind, we'll work down with Bryon and work our way back. Take about a minute to share what you think the next emerging profitable market is for space domain awareness for each one of your business entities. In space, as this crowd knows, the vast profit made from space is made on communication satellites. It drives the industry. It's upwards to 85% of the revenue, and it generally comes out of GEO, up until about three years ago. We have some business dynamics that have changed, but what will be the business dynamics that cause innovation in your domain and your business entities for space domain awareness, or will it just be government procured?

Bryon Kroger:

I think the, again, software is going to power everything, and today it's very difficult to get software onto embedded systems. We've solved the very software intensive web-based applications, UDL, those kinds of software problems. We found ways to quickly get software into production for those. The next wave that I see is similar to the Starlink story that I shared, is how do we create that same path to production for embedded software, including embedded systems that are in orbit. Sending those over-the-air updates. There's a lot of technology that's already available. It's making it work in the DoD and aligning it with the continuous ATO and the path to productions that we've done in more software intensive systems. That's where we're focusing a lot of our effort.

Pablo Pezzimenti:

I'll just say that profitability is a relevant term, and I think we're certainly interested in ensuring that we're ahead of adversaries and making sure that we're delivering the kind of solution that you guys

need to do that. Sometimes that's not the most profitable solution, but it's the one we're interested in delivering. As we think about the future though, we're focused on GEO right now with dark and a few other things, but cislunar is not that far away. We chatted a little bit about that as we were preparing for this, and you shared it wasn't the closest alligator to the vote. I agree with you, there's a lot to do before we get to cislunar, but we are investing today to make sure that we're ready for when the time comes. Cislunar is not that far away, in my view.

Dr. Michelle Parker:

Yeah, and I would say in this rapidly evolving environment, becoming more and more populated, certainly the ability to understand the environment from both the commercial and government side is going to be a key market. I think that looks like rapid deployment of capabilities. I see that becoming much more a way of how we do things, whether that's small satellites, medium satellites, but we're very focused on our Millennium Subsidiary and setting up the production line there so that we can have rapid small sats coming off the line and build on what we did for VICTUS NOX of taking a bus, a spacecraft off the line, putting the right payload on it and getting it deployed rapidly. I think that's going to be a really big area for us.

We're focused on getting that small set factory up and running so that we can deploy the capability that's needed at the time that it's needed as we continue to understand the threats and look to really close those gaps that we have.

Maj. Gen. Gregory J. Gagnon:

Well, thank you for your time this morning. I'll just wrap it up with a theme that ran through the books that was sitting on my nightstand. In World War II, we were successful, and a lot of us have watched movies like Saving Private Ryan, and they focus on the courage of the American Soldier, Sailor, Airman, Marine. But the key tenet in our success in World War II was our ability to outproduce the adversary. We outproduced the adversary because of a restructuring of our industrial base that allowed us to be successful. In great power competition, this is our space industrial base. We will need you, we all need to be rowing in the same direction. Thank you for your time this morning.

Dr. Michelle Parker:

Thank you.

Pablo Pezzimenti:

Thank you.

Bryon Kroger:

Thank you.