Center for Strategic and International Studies

TRANSCRIPT

Event

"DAPA-CSIS Conference 2023: ROK-U.S. Defense Industrial Cooperation for a Resilient Global Supply Chain"

Public Panel: ROK-U.S. Government-to-Government Policy for Building a Reliable Defense Supply Chain

DATE

Thursday, March 16, at 11:15 a.m. ET

FEATURING

Mr. Michael Vaccaro
Principal Deputy Assistant Secretary of Defense for Industrial Base Policy

Mr. Yoon, Changmoon
Director General, International Cooperation Bureau, Defense Acquisition Program Administration

Mr. Pat Mason
Deputy Assistant Secretary of the Army for Defense Exports & Cooperation, U.S. Army

Mr. Karlton Johnson
Chair of the National Space Society, and former Chair of CMMC-AB

Mr. Cho, Junhyun
Director, Director for Defense Acquisition Innovation, Defense Acquisition Program Administration

Mr. Han, Seung Jae
Director, Global Defense Business Division, Korea Research Institute for Defense Technology Planning and Advancement

CSIS EXPERTS

Mr. John Schaus
Senior Fellow, International Security Program, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Mr. John Schaus: (Off mic) – our presenters and panelists for our second session, on "ROK-U.S. Government-to-Government Policy for Building a Reliable Defense Supply Chain." And as we heard in our first session, while this topic may have been a back-burner issue for many people pre-2020, it has since jumped to the top of almost every single discussion we have. And so I'm happy to be part of trying to illicit insights and figure out how to pull us forward in that regard.

And fortunately, we have two excellent panelists and presenters, followed by four very well-positioned commentators. I will introduce first the presenters, and later we will get to our panelists and commentators.

So, first, we have Mr. Yoon Changmoon on my left. He's the director general, International Cooperation Bureau for the Defense Acquisition Program Administration of the Korean Ministry of National Defense. And there he leads the bureau responsible for formulating policies concerning cooperation with international partners and allies. He oversees efforts to promote international engagements to facilitate defense and industrial partnerships with foreign governments.

His bio is extensive. He's had many leadership roles. I won't go into each and every one of them, but a quick taste. His responsibilities include contracting and management of FMS, foreign military sales, with the United States. He has previously led the DAPA Robot Program team, the main battle tank program, and the advanced technology program. He is very experienced in this area and we are looking forward to his remarks. And potentially of most interest to some of us in the audience, he was here at CSIS a number of years ago. Is that correct, Mr. – yes. Welcome back. (Laughter.)

So briefly, following Mr. Yoon's presentation, we will hear from Mr. Vaccaro again, Michael Vaccaro, who is, as you heard earlier, the principal deputy assistant secretary of defense for industrial base policy, an increasingly critical role as we are looking to the future. And he was very well-introduced earlier, but in case you're just joining us, he leads the Defense Department's efforts to develop and maintain the U.S. defense industrial base and to ensure secure supply of materiel critical to national security. He's held numerous senior positions in both the Defense Department and in the Commerce Department, before, as I understand it, a career engaging with Koreans from the outside as well.

So with that, let me turn it to Mr. Yoon for your presentation. Thank you very much.

(Note: Mr. Yoon's remarks are made through an interpreter.)

Mr. Yoon Changmoon: (Inaudible) – like just explaining, I was a visiting fellow to CSIS. So it's, like, five years ago. And I can see that during that time there was a lot of issues in

the international stage, and a lot of changes. In this important time, I'm going to – I am here to talk about this important topic today. So today we're going to talk about evolving global defense industry landscape, ROK-U.S. cooperation in defense procurement, and ROK-U.S. cooperation in cyber security, and also the roles of each stakeholder.

First of all, the evolving global defense industry landscape. Basically, the defense industry is about having limited suppliers. And on top of that, from 2020, due to COVID-19 pandemic, there were crisis of supply chain. And last year there was this war in Ukraine, which is ongoing, which makes this supply chain crisis a more realistic crisis to us. Last year in May there was this bilateral summit meeting.

And in order to strengthen our strategic alliance, we are going to do – the two countries agreed on reinforcing the bilateral partnership. First of all, I'm going to talk about supply chain policies between the two countries. As Mr. Vaccaro just mentioned, the United States has issued a lot of policies for supply chain. What's in particular, the United States not only internal development, but also it is stressing ally-shoring, for example, like cooperation with allies and partnerships.

Next is Korea's supply chain strategy. Korea's supply chain policy is mostly focusing on cooperation with the United States. First of all, in the procurement area we are reviewing entry into SOSA. And, secondly, in the cybersecurity area, we are – based on the CMMC of the United States – we are preparing K-COMMC. And also, in the advanced technology area we are trying to participate in FCT and also have cooperation with the United States in military semiconductor and space.

So first of all, I'm going to talk to talk about the status of Korea in terms of SOSA that we are reviewing right now. SOSA, this arrangement, as you can see from its name, it is a part of the efforts to have security alliance and also supply chain cooperation. It is mostly about guaranteeing the mutual supply of goods. It's not legally binding, but it is going to be very effective. It is going to be signed between the United States DOD and DAPA. And currently the United States have SOSA with 12 countries.

So these are the key contents of SOSA. So it is about having priority on some certain contracts. Then the counterparts will support the other country so that you can have implementation of priorities. Through SOSA, the two countries can ask for timely delivery and get support on that. The United States has deep past with just the existing system. And Korea does not have such a system currently, so currently also the DAPA and the promotion agency can have CoC to support priority. And industries of Korea can voluntarily participate in this arrangement. Through SOSA signing, we think that our partnership will be reinforced. And also the companies that

participate in this arrangement will be recognized as trustworthy suppliers. So it will be a good opportunity for them to also participate in the global supply chain.

Next ROK-U.S. cooperation in cybersecurity. Currently the United States, targeting 2026, is implementing cybersecurity certification system, which is CMMC. The United States not only the prime companies participating in the acquisition project, but also international companies also required – are required to have CMMC. It has five rays and is going to be revised this year as CMMC 2.0. Based on this, for Korean defense industrial companies that are participating in many acquisition projects of the United States, CMMC is a must. As a representative case, the F-35 and FA-50, CMMC is very important to have contract with DOD.

Fortunately, the Republic of Korea has made a lot of investment in defense industry technologies. Under the name of Integrated Survey – in the name of Integrated Assessment, actually, it has evaluated 1,226 items in six areas every year. This Integrated Assessment not only is about information protection, but also technology management and military confidentiality. Based on this assessment, Korea will also try to include items from CMMC to establish so-called K-CMMC. More specifically, in 2026, before the all-out implementation of CMMC, we're trying to establish K-CMMC to have mutual recognition with the United States.

The U.S. DOD also announced that it will pursue mutual recognition with CMMC with foreign cyber security system. So we can look forward to mutual recognition of K-CMMC and CMMC of the United States. Through that, internal in Korea, like, domestic companies can have more credibility and also it will open more opportunities to participate as contractor to acquisition project of the United States. Ultimately, among allies, we will be able to minimize overlapped investment so that we can secure more time and resources.

Next is ROK-U.S. cooperation in military semiconductors. Korea is a world-renowned semiconductor powerhouse, but we are still lagging behind in terms of DIMM memory, which is important for the military industry. Due to the recent crisis, there is this unit price increase, and crisis in terms of the supply of semiconductor. DAPA, in the cycle of this year, will establish a development strategy of military semiconductor. And it will pursue plans to secure technologies and nurture industry for weapons system.

From 2023 to 2027, we will identify important and major semiconductors, and we're trying to secure relevant technologies. And from 2028 until 2032 we will pursue onshoring for critical military semiconductors. And from 2033 to 2037, we will try have self-reliance of semiconductor in the military area. And we're trying to have also the IP to secure advanced technologies.

And for such development plan of Korea's military semiconductors, it is essential to have cooperation with the United States.

In terms of technology infrastructure investment, the United States is number one in the world. So if Korea will – for Korea it is very important to have benchmarking of the United States, but more than that what's really important is the capabilities of the United States and also Korea's strength in the memory semiconductor. Through that, we'll be able to have a win-win strategy. And we're trying to propose that. If we can share technology development roadmap, and if we come together to join R&D in this regard, I think we can have better results.

Like I just mentioned, to implement such policies there are roles for each of the stakeholders. First of all, the government. The two governments already have a lot of devices for implementation of such policies. DTICC, DICSC and TCSC. There are many entities to implement such policies. In 2023, the – like SOSA, CMMC, and other military semiconductor-related cooperation policies can be discussed. And we look forward to see that we see agreements in this regard.

Next is industry and academia, including the civil think tank, like CSIS. While companies of the two countries already have strong partnership, however I hope this can be an opportunity for us to accelerate such partnership, and also, like CSIS, the, like, civil think tank is very important. This third-generation partnership was the agenda proposed by CSIS. And this is now reflected in the two countries' major policies having actual impact, as we see. Like I mentioned, there's SOSA, CMMC, and, like, military semiconductor cooperation.

We have made a lot of progress in terms of, like, our discussion with DOD. Some of them are just at the stage of idea sharing, but what's for sure is that the two countries, based on our alliance, we are going forward to make a trustworthy supply chain. The current global security environment will emphasize the need for our alliances. Under this environment, Korea will do our best to become a trustworthy supplier. Thank you.

Mr. Schaus: Mr. Yoon, thank you very much. That was an excellent presentation, and you've given us a great deal to think about as we launch into this second panel. Thank you very much. Please join me in a round of applause. (Applause.)

Mr. Vaccaro.

Mr. Michael Vaccaro: I'd like to use Mr. Yoon's slides. It'd be perfect for me, because we could do the discussion. (Laughter.) No, I'm happy you went first, because that's really going to help me sort of frame some comments. But I'm also happy that

someone read our report from last February, because I recognized the four "I's". So I was very happy to see that. But, you know, I think a lot of what you hear me speak earlier is relevant to today's discussion – this panel's discussion. But let me just kind of maybe zero in on a couple of key points that Mr. Yoon raised, and maybe elaborate a little bit more on what we're thinking.

One is on the security of supply arrangement. And I think during the coffee break I had an opportunity to chat with several people here. And I think I may have highlighted that I've been championing of having a SOSA with Korea probably for about 15 years. And so I'm really excited that we're getting very close to finalizing one. So, you know, if you look at the idea of a SOSA, the United States has had a longstanding security of supply arrangement with Canada, which actually dates back to 1950. And it just makes sense, given the integrated nature of our defense industrial bases.

The other SOSAs really started to appear in the early 2000s. And so actually we have 14 of them right now, because we just signed one with Israel two weeks ago. And I think it was just really evident that in the early 2000s, as there was consolidation in our defense industrial base and in Europe, you know, we felt it was necessary to have mechanisms in place that indicated – partly to prevent fortress Europe from happening. We didn't want Europe to feel like they should just rely on European suppliers. But we also recognize that we're big governments, an in the event of an emergency where you experience a supply chain disruption, it could actually take a while to find the right people who could potentially help. And that's one of the benefits of having a SOSA. You have designated points of contact.

So I'll tell you the experience. We had a folio of arrangements that we negotiated in the early 2000s or mid-2000s, largely with Western European countries. Then there was a pause. Then you see a surge of additional ones. And a lot of those were related to countries recognizing the interdependences of our supply chains in the context of Iraq and Afghanistan. And there was a lot of countries who were relying upon U.S. suppliers and were having difficulty getting spare parts for their systems, especially if they were U.S. origin. And that's why you saw the flurry of activity.

And then there was sort of a pause. We hadn't done one – Norway was the last one we had done up until recently. And I think that was in 2018. And then, as I mentioned earlier, as part of our supply chain report we really highlighted that we felt that SOSAs were being – we needed to have more. And so we've had a second wave, if you will. And Korea is part of that second wave. And I'm really hopeful that we can conclude an arrangement with Korea soon, in hopefully the coming months, and additional partners. We're talking to several other countries right now.

But, again, it's just an important mechanism. And I tell stories, so I'll tell a story. I was visiting with a Western European country. And this was when operation in Iraq were pretty hot. And this is with a partner that we already had an existing security of supply arrangement with. And it's the night before we're having our full bilat meeting. We're having a dinner. And I'm sitting across from my procurement counterpart. And I ask him: Are you having any specific challenges in your procurements? And he says, oh, yes, we are. I'm trying to get spare parts for this U.S.-origin aircraft. We got aircraft on the ground. We're supporting you downrange. And I've been trying to solve this problem for three months.

And he's telling this story and, it's, oh, and it's going to be raised at the four-star level. There's going to be a call. And I'm like, aren't you my security of supply counterpart? And he said, yes, but I'm new in the position. What is that all about? And so this poor guy had been trying to solve this problem on his own for months. And once he discussed the challenge with me, we were able to solve the problem and get the items delivered to what they needed in less than two or three weeks. So it's an example not only is it important to have these mechanisms, but to actually have that personal contact and have people understand what the benefit is.

So I think another huge benefit of having this SOSA, and it builds on the theme we talked about earlier – how you can help encourage industry-to-industry cooperation among our industry – is, as Mr. Yoon's highlighted, it signals that Korea and their companies who sign the code of conduct want to be reliable suppliers to us. And so, you know, and what we'll do – and I look forward to having opportunities to engage with KDIA, which I've met with, supported meetings in the past.

But let's leverage those – our trade associations. And KEI in particular, you know, to highlight what capabilities Korean industry may want to highlight to help satisfy U.S. requirements or to help support the U.S. supply chain writ large. And so it's also an opportunity not only to have designated points of contact to respond to urgent requirements as necessary, but it's also an ability for Korean industry to highlight – another forum for them to highlight their capabilities. So I think that's going to be really good.

I should also say that, you know, even without a security of supply arrangement, if the Korean government or Korean industry is experiencing challenges today in getting timely delivery of equipment from U.S. suppliers, we do have mechanisms today – we are actually working on a couple of examples now – where we can actually authorize Korea and your industry to use our DPAS system, which gives priority. But having a SOSA just makes it much easier and quicker from an approval process from our side. But if there are challenges today that are emerging that you need assistance with, don't

wait for the security of supply arrangement. We can help address them now. And there's folks in DAPA who know how to do this, and our embassy team.

On the second topic – or, on the third topic, I guess – on CMMC, this kind of builds upon, you know, the key enablers that we talked about earlier that from a cyberspace you're only as strong as your weakest link. And CMMC was an initiative started in the last administration. And, you know, they recognized that, you know, we needed to do more on cyber. And this administration, the Biden-Harris administration, has also recognized that. But there was a lot of industry concerns that was highlighted about CMMC 1.0. And so when the new administration took office, they directed a review of the CMMC approach. And there was a recommendations and findings share with Deputy Hicks. And that's when the decision was made to pursue what we're referring to as CMMC 2.0.

And A&S had been the lead for CMMC 1.0. Dr. Hicks made the determination decision, and it makes a lot of sense, to actually move that responsibility to our office of the chief information officer. So right now, my team is not involved in the development of CMMC 2.0. It is the responsibility of our chief information officer. And I know they are in the process of drafting a rule. What I will say, is it's my understanding that this rule will be published as a proposed rule. And what that means is that when we publish the rule, it'll be published for comment by industry and the public writ large. And it'll be published in our Federal Register, which comes out every day.

I will encourage industry, both U.S. and international, that when that rule is published, is proposed format, to review it closely. And if there are things that work well, highlight that in the comments. We welcome comments. But if there are areas of concern, I would encourage you to acknowledge those and submit comments on those. I will say, I mentioned earlier in my remarks that I was heavily involved in export control reform in the Obama administration. And that was, you know, a multiyear effort to transfer less-sensitive military items from State control to Commerce control.

And what we have found to be critical to the success of that initiative is that we publish proposed rules for every category that we were trying to transfer, to make sure that what we were proposing made sense to the regulated community. And in that case, it was industry. And it was U.S. industry and foreign industry. And I will say that the comments under our rulemaking process, we have to seriously evaluate and address any comment we receive from the public as we develop our final rule. So we cannot just ignore a comment.

And I'll tell you that that rulemaking process helped ensure, I think, that when we did go final for the various categories, export control reform, that we developed a new system that was capturing what we wanted to capture,

and could be enforced, and complied with by industry. And I will say that in a couple of categories, the comments we receive from industry were so enlightening that we went back and had to publish another proposed rule before we went final. So again, just to stress, that sometimes you – industry has an opportunity to be part of this process. So I encourage you, once it is published, to take advantage of that opportunity.

We talked a lot about semiconductors. And obviously Korea plays a leading role in semiconductors. And some of you – the Korean semiconductor leading manufacturers – have met with our senior department leadership in the recent months. I will say, that's a great example of a sector where the Department of Defense is not the leaders, right? We account for probably 2 percent of microelectronics consumption in the United States. But what we need is really important to our weapon systems, right?

And, you know, one of the things I – you know, I don't think people appreciated so much last year, and it started really with Javelin and Stingers. But folks didn't understand why we couldn't just start producing, you know, vast amounts of these weapons within weeks. And, you know, on good days – we'll use Javelin as an example – you know, good days it probably takes 18 to 24 months to make a Javelin system. But these are complicated machines. These are not – you know, folks have a tendency to think of the movies during the reporting on World War II, where we were pushing, you know, shells by the hundreds of thousands through assembly lines. The arsenal of democracy, you know? But, you know, these are highly complex machines that have hundreds, if not thousands, of semiconductor or microelectronic components in them. And so that's critical.

And so the challenge that we really have as a Department of Defense is, yes, we need the state of the art future semiconductors. But we also need reliable suppliers of legacy chips because our systems are going to be in our inventory for a long, long time. And you want to make sure we have that capability. So that's sort of, as we're working together as a whole of government approach with our Commerce colleagues, and Energy, and other colleagues, as part of the CHIPS Act, that we want to make sure that we're considering the important national security implications and requirements that we have going forward.

I know that I think that during one of your last conferences Dave Honey, from our research and engineering, participated. And Dave is one of the leaders in the department on working the microelectronics challenges. The other leader, from A&S, is actually Dr. Chris Michienzi, who's going to participate in the panel this afternoon. So she's really been our point person for implementing the CHIPS Act. So I'm sure you'll have a lively discussion with her this afternoon on that. But again, I think, going back to our fundamental strategy on the supply chain and microelectronics,

international is key, working together with our allies and partners. Government and industry. And so I'm happy you raise that as an area.

You also highlighted – (off mic) – the DTIC, which unfortunately really hasn't met. I think the last time there was a face-to-face meeting was in 2018. I've been with the department since 2019, and unfortunately I arrived, and then a few months later, or a year later, we had COVID. And we weren't able to have – squeeze in the DTIC before that occurred. But I will stress that, you know, I think that Dr. LaPlante highlighted it during our meeting with the minister on Tuesday, but we look forward to hosting this meeting in the coming months in Washington. We look forward to it.

And my understanding is our teams had a good discussion yesterday, and are building a robust discussion that will sort of highlight a lot of what we're trying to – areas where we want to cooperate going forward, but also from the supply chain standpoint, you know, sharing lessons learned. We've learned a lot based on the experience in the past year with Ukraine. And we look forward to sharing lessons learned with Korea and other countries around the world, and with NATO. So and also, I think that – I'm happy that R&E was able to have their TSE meeting in the fall. And the readout I got from that, that it was good and there was sort of revitalizing of that workstream, which is critical too.

So I think if you're looking at it from, like, a – where we have the DTIC, where we have the robust discussion on defense industrial base cooperation, but we're also revitalizing the government-to-government both S&T-type cooperation, but hopefully that will lead to broader co-production, co-development, and other cooperation in that space. But again, I also want to highlight that I think we should also – we can leverage the industry-to-industry forums, and look forward to receiving input – and academia – for suggestions on where we should – what are win-win opportunities.

But I'm very optimistic that we're set to have great success this year, both at the government-to-government side, but also at the industry-to-industry side. And also in the FCT program, I'm really happy that you highlighted that. My understanding is I think there are five active FCT programs – foreign comparative test programs – involving Korean industry today. And actually, one of the Korean industry reps came up to me today. He was actively – he was one of the projects that are active. So again, that's a great example of us leveraging both of our industrial bases.

So look forward to the rest of the discussion on the panel. Thank you.

Mr. Schaus: Thank you very much. So those – (applause) – yes. Please join me in a second round of applause. (Applause.) I think what we have before us is already a very rich set of issues, building off of the first discussion and now these two

presentations. But before we start diving into those questions, I think we have even more to put on the table. And to help us do that, we have four superb panelists, who I'll introduce very briefly. And then we'll go, I think, Korea, U.S., Korea, U.S., through the panels.

So quick introductions. American, to my right, Mr. Karlton Johnson, colonel, United States Air Force, retired, is the chairman of the National Space Society. And in that role, he's the chairman of the society's board of governors. And he provides strategic and senior executive leadership to the board of governors in support of the society's goals and serves as a primary spokesman for the Space Society's board of governors. In 2014, he retired from active duty in the Air Force after 26 years, where he held a variety of senior leadership and command positions within the U.S. Air Force. Look forward to hearing your comments, Mr. Johnson.

And to my – well, let's go Americans, and then Koreans, and then we'll go around. So Pat Mason is the deputy assistant secretary of the Army for defense exports and cooperation. He is the Army principal responsible for security assistance and armaments cooperation. I've been out of government too long. These words are no longer flowing off the tongue correctly. He also manages export policies, direct commercial sales of U.S. Army defense articles, and international cooperation, research, development, and acquisition. He has held numerous roles – senior roles, managing and overseeing programs within the military – or, within the Army, particularly on the aviation and missiles side of the house.

For our Korean colleagues, we have Mr. Cho Jun Hyun, director for defense acquisition and innovation in DAPA. He has previously served as the director of finance and director of defense industries job division. And, like Mr. Yoon, he was a visiting fellow here at CSIS. So I'm noticing a trend line. Thank you and welcome back.

And finally, but not least, Mr. Han Seung Jae, who is the director of global defense business division at the Korean Research Institute for Defense Technology Planning and Advancement. There, he has held – well, over his career he has held numerous positions of responsibility in the Korean Army, in the Korean government, and in Korean industry. So providing a well-rounded perspective that we look forward hearing from. In the military he was an army officer. He served in defense industry in several advisory roles to Korean corporations, and has worked international cooperation within the South Korean Ministry of National Defense.

So if I could, I'll start, Pat, with you. And then we'll go next to Mr. Cho. All right.

Mr. Pat Mason: Well, good morning. Almost – I think it's good afternoon now. So good afternoon. It's a pleasure to be here. And thanks to CSIS for having an Army representative. And hopefully I can provide a little context in just a few brief remarks on how you move from policy down to implementation, and how at the service level we are implementing the things that Mike has talked about, and how that has played out really over the last, I will say, 18 months, and some of the critical actions we've had to take. But really, how that goes forward to what we've discussed earlier today. And, Minister, you talked about this third-generation approach to our cooperation.

So if I take a step back, I know in the introduction it talked about what we do, but it is unique because we span between our A&S colleagues that are at OSD, the R&D colleagues at OSD, as well as Director Hursch, and the director of security cooperation. And so in doing that, it's really the security assistance FMS, it's armaments cooperation and collaborative science and technology, it's foreign comparative test, it's tech security and foreign disclosure, it's the licensing and export piece, in conjunction with our colleagues. And then it's also the technical exchanges. And in fact, we have three technical exchanges right now between Korea and the United States in the area of medical and then really artificial intelligence. And that's a program that we orchestrate on behalf of our science and technology community.

So when you look at that, I wanted to make some comments just on how we are moving forward in a number of different areas. And obviously the backdrop of that is the tremendous challenges that we're having in supplying what is necessary, and the realization of the issues within the defense industrial base, where we don't have the resiliency and the responsiveness. So Mike's example of Stinger and Javelin, usually Army examples are brought out because of the amount of materiel that has been provided to Ukraine. But then also, as we've looked at global demand, land forces have been a renewed interest in, quite honestly, things that had gone, I'll say, out of vogue. Armor formations, artillery, rockets, and then your munitions depth.

Those land forces elements we had leaned down. And I will say that I was part of that process as a former program executive officer. What I was very lean, multiyear contracts on our aircraft, lean supply chains, and price points so that we could buy at quantity in many cases. And what you sacrificed on that was the robustness of the industrial base, multiple suppliers, and then the ability to have a resilient supply chain that gave you the opportunity, when you had disruptions, to quickly recover. Or, it really gave you the surge capability that is necessary.

And so certainly working for the Honorable Doug Bush, who's the Army acquisition executive, he is my boss and we are underneath ASA(ALT). This is a focus area of his. And it's really a focus area not just for the United States

Army so that we can equip the Army, but also for all of our international partners. But it is clear and, as we've seen play out in Ukraine and in the security environment, that it is by, with, and through allies and partners that we execute all of our operations in the future. And so you've really seen a very, very large shift within the Department of the Army over the last, we'll say, 24 to 36 months. And I, consequently, get a lot of help from everybody these days as we look at our relationships with allies and partners.

And so with that as a little bit of a backdrop, I also want to put the challenge forward of what we're doing in the Army from a modernization perspective. And so as the Army is doing this, and we have to look at resilient supply chains for the systems that exist today, the Army is executing a massive modernization effort. Whether it is next-generation combat vehicles, long-range precision – long-range precision fires, integrated air and missile defense, or future vertical lift, as we modernize to those systems, we are taking the lessons that we've had in the past and looking for how those can go from collaborative science and technology work into collaborative development, collaborative production, and then how we manage supply chains collaboratively as well as do sustainment activities collaboratively.

And I will say, CSIS has played a critical role in that as we looked at things that improve for exportability, such as open-systems architecture, and how we integrate that into our combat vehicles, aircraft, and artillery systems. Because the research that was done on that and how we change the business model associated with that is critical to ensure that we have exportability in the designs as they evolve, and then also really what that plays out to is interoperability. Because that is what we are ultimately interested in, so that when we have multilateral operations that we have interoperable forces that can execute – should they be called to fight can execute a fight.

Or, in defense, deter forces because of the interoperability that we collectively provide within an integrated security environment. And so from a tangible perspective, on the armaments cooperation front, while we haven't had those meetings since 2018, we do have a number of science and technology efforts that are going on right now. In fact, seven total. Which doesn't sound like a lot, but these are robust science and technology collaborative work, not just data exchanges. And we have two more in development.

And certainly the – I'm going to say the hope out of this – but the methodology that we're looking at is not that we simply collaborate on science and technology and then we go in separate directions. Rather it's how does that lead to co-development of systems or subcomponents, elements that can go into systems that, again, ensure that interoperability? And then how that leads into production opportunities throughout our allies and partners, where that is shared. And we certainly see the need for that.

And then the last aspect of that, that I talked about earlier, is how that leads into the sustainment side of the house.

And so with that, from that S&T working group that we have, we are also underneath the DTIC and the TCSC, and all of our nice acronyms that we have, we are also starting a logistics working group, because we feel very strongly that we have to have a strong logistics component, and look at how we do repair and returnables for both the ROK and for U.S. forces, as well as regionally within the INDOPACOM region. That's critically important. And so that's really the next step that we're taking.

The last comment, and I know we're given, maybe, five minutes so there's a number of different areas I can talk about. But I did want to talk just on supply chain, because the one thing that we did realize, and certainly OSD, the policies that they went out, is we really do not understand the depth of our supply chain. And it started in COVID. And I was a PEO at the time. And so what I realized from that is because of the nature of our supply chains and the disruptions that we had due to the pandemic. We really need to have illumination on it. There's certainly a number of tools. There is an industry component to that. There is a government component to that. And it requires significant collaboration.

And so that is the area that we have worked extensively on. And again, I'll highlight work by CSIS because of the aviation side, where it looked at the aviation industrial base, and it looked where it collapsed down to fragile suppliers, where we needed to go and do targeted investment. And so that is the opportunity with allies and partners as we work forward and we really explore our supply chains, to understand where those fragile suppliers are, how we reinforce that by having opportunities for greater growth for businesses to participate in that, and then how we can have that secured source of supply.

And so that's a tangible example of how we went down and identified the areas that we specifically wanted to target with industry, and then really looking at industry to take that lead and figure out how to diversify or build that supply base. And then the last thing that I will say on CMMC and the cybersecurity aspects is it is a balancing act as we go out there, because we want to entice small businesses. One of the areas that Mike had talked about earlier is the fact that we have a number of small businesses that are not participatory anymore.

And I will say, on the Army side, within the small business innovative research, we've actually standardized and streamlined the contracting process so that they have to learn it once, it doesn't have a lot of overhead because these are very, very small businesses. And so how we do that, because we have to have cybersecurity built into our supply chains. We

know that. And that's why it's going up for public comment. And so that's an area that we are also working on within the Army on how do we actually implement that with industry and also ensure that small businesses can be participatory in that. And that is a – that's a tough road to navigate. And that, to me, is one of the bigger challenges ahead. So thanks very much.

Mr. Schaus: Pat, thank you very much. That was outstanding. And I would just like to say, on behalf of my colleagues Cynthia Cook and Greg Sanders, who led much of the work that you referenced, it's always good to hear that the work is reaching people who are listening. So thank you.

Let me turn now to Mr. Cho Jun Hyun for your comments.

(Note: Mr. Cho's remarks are made through an interpreter.)

Mr. Cho, Junhyun: Yes. Good morning. I was at – I was a visiting scholar here in 2019. And that was a great experience for me personally. Currently, I am the global defense business division director. In fact, for the case of Korea, we have Samsung, SK Hynix, and other memory-related big players. And they have great technology. And they have global competitiveness. However, for those memories that can be applied to the weapon system, those are all non-memory chips, mostly. And the system semiconductors are generally used for the weapon system.

But this area, Korea doesn't quite have technology or competitiveness in this sector yet. For these semiconductors for the weapon system, they have to be operated under extreme conditions and have to have high reliability. And for the 20 to 30 years of the weapon system life cycle, the semiconductor has to be supplied to the weapon system to be viable option. And Assistant Secretary Vaccaro just said profitability of these items are generally low because the quantity is very low. So it's hard to have a scope of economy – economy of scope for this matter.

And what also matters is the security and maintenance of security. So how to deal with the security is what we need to think about. And for the system, semiconductors, interfaces, and other software-related connectivity and interoperability are all very important factors. So we have various obstacles to overcome. When we deep dive into the semiconductor sector, unlike the other items, the production process is very complicated. And production is very divided. For instance, fabless and post-fabless design and IP foundries, packing, all these are one of the processes, and very complicated and divided.

So one company cannot handle the entire process, which is a special characteristic of the item and industry. That is important factor, but for us AI – which can be connectivity to the unmanned systems, et cetera – all these

developments when they're developed together the system semiconductor can also develop alongside with it. Otherwise, it'll be on unbalanced, which will be a problem for us. So we are at the beginning stage of the policy for these items. But by the end of this year, the ROK government is trying to have a bird's-eye view of our strategy and policy on this.

And we need cooperation with the U.S. in this sector. It's critical. For the case of the United States, assistant secretary mentioned in his remarks the market share of the DOD in that sector is 2 percent, and the quantity is quite low. Because of the low quantity, it's hard to have a proper production and proper supply chain. And that's what I can easily predict because that's what we're thinking in Korea as well. That's why we need cooperation between the two countries, and especially in the R&D sector. So through the joint R&D we can jointly develop a chip. So if we have joint standards and work on it, that can drive down the costs a lot. And we can have a very cost-effective mass production and overall productivity and production efficiency later on.

To some degree, when we're establishing strategies and roadmaps, I think we need to share our roadmap and strategy so that we can have a good direction for the two governments to go forward. Lastly, overall, the tanks and aircrafts and all these final items, that's not what we're talking about. We're talking about the lowest-tier items. With that, we need cooperation between the traditional defense businesses, but we also need cooperation between the defense industries and semiconductor specialty companies, in case of Korea. So we need to have a variety of channels of cooperation. And we have to reorganize that cooperation system. Thank you very much.

Mr. Schaus: Thank you. That was a great dive into the specific challenges we face in the cyber realm. So thank you very much, Mr. Cho.

Karlton, please, over to you.

Mr. Karlton Johnson: I'm probably going to mess up the translator, so I apologize for this.

(Continues through interpreter.) Colonel Johnson, thank you very much. Thank you for inviting me. I love Korea. Let's go together.

(Continues in English.) I want to say to all my brothers and sisters out there from Korea, I do love the Korean people. My father fought in the Korean War. My youngest son was adopted in Korea. And I had the opportunity to serve with some great leaders, some of them who are here today.

And one of the things that I got to understand while serving in Korea was the threat that you have to deal with from the North is a lot different than what other nations, I believe, have to deal with. For example, when we talk about things like cybersecurity and cyber risk in the United States, and when we

have a cyberattack on something like our pipeline – you know, very significant. Causes problems. But the adversary is not seen, the effects of the adversary are seen. However, when you have a cyberattack in Korea that happens to come from, say, North Korea, you have 35 kilometers or so between you and potentially the next war.

So while serving in Korea, I had the opportunity – and I will say I was given the opportunity by a gentleman called General Thurman. If you've ever seen General Thurman, he's a very intimidating person. And during our first session, he was giving an update on an exercise we were going to do. And he asked specifically: What are we going to do about the cyber threat? And there was silence at that moment. And he looked around and he said, where's my J-6? And I was his joint – the J-6. So I pressed a button. And I said, sir, Colonel Karlton Johnson, J-6, at your six o'clock. General Thurman turned around and looked at me.

And this big gentleman got up and said: You're not an Army guy. And I went, no, sir. I'm better than that. And he said, you know, you don't want to end up on the hood of my car, all right? I said, sir, I won't be that guy. You're going to have great cybersecurity. And right after that, I got with the J-3 and the J-2, the intel and ops, and said: Gentlemen, I think we need to build a cyber capability, like, really quickly. Because that's not going to be me on his hood. And through that effort, we were able to create the first joint cyber center, that was the only cyber center that was a sub-unified command joint cyber center.

And I had the opportunity to hand-deliver the first cyber intelligence to my ROK counterpart, the ROK cyber commander. He and I were on speed dial. So I got to very up front understand the cyber threat. And because of that, when I transitioned out of the military and had gone into the public sector, in addition to serving as the chairman of the National Space Society, I have a practice that does cyberspace development and also C-suite advisory in AI ethics development. We also – I had the opportunity to become part of the CMMC effort.

The thing I'll say about CMMC, and we'll talk about that a little bit more, is imagine this: A situation where we know that the supply chain is at risk, but you want to have industry be part of that solution. You call industry together, and you say: Help me solve the problem. A group of seven people get together. That seven people are asked to create a company, that company has to be a nonprofit to work this problem. Zero funding – repeat, zero funding. But you have to support 375,000 companies in the defense industrial base.

So we went from zero to hero in a COVID environment. That's a remarkable accomplishment. And I want to applaud the men and women who stepped

up to do that, and Matt Travis, who's now the CEO of the now Cyber AB is leading that effort. But here's the challenge when it comes to something like CMMC. CMMC, regardless of if you're using something like zero trust or whatever discipline, it comes down to understanding and accepting risk. And part of the challenge with small- to medium-sized businesses is that they've had to carry this risk a long time, but they chose not to accept that fact.

And that's why, under the – what they call the NIST 800-171 criteria, which if you have a government contract you're supposed to do anyway, people were not doing it. So CMMC is really a lever to encourage and emphasize and validate whether or not you're doing what you're supposed to do. In Korea, you have an opportunity to do a CMMC-like environment. You may not do it exactly like the United States does. And that's up to you. There's a lot of opportunity to evolve it in a way that works for you. But you have more of a prerogative to do it, because of the threat and how pervasive it is for you.

So I would recommend as we're talking about this you look at not only implementing it, but implementing it in a way that works for you, and leveraging on the successes and the challenges that we've seen in the United States. The last thing I'll say about that is as we talk about, again, small business and large business, again, it's not a matter of if, it's a matter of when you're going to get cyberattacked. And here's something that keeps me up at night: It's not an attack on my national infrastructure. I feel that we have great men and women serving in powers – serving at levels of power and authority to oversight and make sure that that doesn't happen.

What concerns me is the small business who doesn't look at protecting their own IP as well as they would protect anything else. A single part that comes in and is now configured differently, a spec is changed. That spec goes into a weapons system that's supposed to defend the men and women that are defending the nation. And then I see that as men and women dying unnecessarily. And that's something that doesn't happen on my watch, and I hope it doesn't happen on yours. So my encouragement is that you take this opportunity to work with the United States as much as possible, on strengthening your cyber hygiene, and leveraging capabilities like CMMC and zero trust and others to do that.

The last thing and then I'll pass it over, on the space side. I'm putting on my National Space Society hat. In addition to cyber, space is cool once again. And I want to thank guys like Elon Musk and others. But all they're focusing on right now is launch. That's good. That gives us access. We need to look at the entire ecosystem of what we're going to do in space. And countries that are both space faring, like the United States, and countries that are non-space faring or emerging space-faring nations, have an opportunity to figure out how we're going to work together.

Something I'll leave with you as a vignette. Let's say that this is an asteroid and your company – one of your companies, sir, goes out, lands on an asteroid, and now they find uranium, or iridium. Another country – I'm not going to say China – comes in and lands on the other side of the asteroid . Who owns the asteroid, you or China? Well, I would submit, that whoever has a bigger gun is going to own it. So we have to have a conversation on what are we – how are we going to operate in space? What are we going to do in space? Where are the potential areas of collaboration? And this is another area that we, as United States and Korea, have an opportunity to talk about, how we're going to kapchi kapchida – (off mic). (Applause.)

Mr. Schaus: We are running very close on time. So before I turn to our last panelist, Mr. Han, I will say if we have time for one or two questions to prepare them now so we don't have a moment of awkward silence and run dry on time.

But, Mr. Han, the floor is yours. Thank you.

(Note: Mr. Han's remarks are made through an interpreter.)

Mr. Han, Seung Jae: Hello. I am from Korea Research Institute for Defense Technology Planning and Advancement, Global Defense Business Division Han Seung Jae. I have also participated in this conference from 2019, not as a visiting scholar but as a participant. Like our director general mentioned, that all the, like, reliable supply chain, TVC, global economies in Korea, I think these can be very important issues, especially with the COVID pandemic and Ukraine War. We have realized the need for trustworthy supply chain partner.

The word "trust" or "credibility" I think has two kinds of meaning to TVC participants. First of all, it is about pursuing common value among the United States and also, like, friendly countries at the level of diplomacy and security. And the second meaning would be about delivery, quality compliance, I mean, in terms of the economic meaning of trust, for the products. To have robust TVC I think it's very important to broaden the horizon of cooperation in the industry between the two countries. In this regard, I think I want to talk about TVC cybersecurity and also military semiconduction in regard to the cooperation plan between the two countries.

First of all, about the trustworthy supply chain, TVC. So I think the companies that can contribute to bilateral supply chain cooperation, I think they need to pursue continuously establishment of database and technology and products. KRIT is leading the efforts for projects on key technology development and product development to nurture our industries, companies, with competitive innovativeness. We have established and managed a database on these companies domestically. And moreover, DAPA,

which is leading the system development project, we are trying to have mutual exchanges of database on the companies that we have data about.

I think such efforts will be helpful in having continuous and immediate cooperation by utilizing such database, by identifying fragile supply chain area. And secondly, as assistant secretary just mentioned, FCT and also FTASS project by the U.S. Army Center as the participant to such cooperation project, we are very committed to participate in those project. Last February, in Seoul, for 27 Korean companies the U.S. FCT team visited Korea and had one-on-one consultation meetings. There were a lot of progresses in this event. And through such events promising companies in Korea are participating actively in FCT efforts.

So I'm hoping that FCT project is not going to become just a testing vehicle. I hope it will become a successful model that will lead to actual acquisition project. And moreover, similarly, if there are projects that the U.S. Army – the U.S. military wants from their allies, we will actively cooperate with you. Thirdly, based on reinforced supply chain cooperation, I think we need to have co-development of weapons system and also co-export and marketing, which is actually, so-called, the third-generation partnership.

The two countries do have a great case, which is T-50 trainer jet, which is gaining a lot of attention globally. As you know, the T-50 trainer jet, which was developed as part of – on the sideline of F-16, is being very successful, being exported to Southeast Asia and Middle East. And we are sharing this successful security results and economic results together with the United States. Going beyond this, I think that the two countries also are allies. In order to respond to – closely to our common threat, we need to have co-research development program for weapon system, and also for export to third countries.

Next is cooperation plans in the cybersecurity area. There is a lot of case of technology extortion in cyberspace. So I think it's very meaningful to have a safety net, such as CMMC. Currently, the United States is implementing CMMC, cybersecurity certification system, targeting 2026 for full implementation. This is necessary not only for the direct contractor participating in the acquisition project of the United States, but also for the subcontractors under them.

Like the international cooperation director general just explained, our KRIT, together with the establishment of K-CMMC, we are conducting specialized training for Korean defense industry companies, so that they can be prepared for CMMC in advance. So that in 2026, when it's fully implemented, we will support our companies so that they can actively participate in the U.S. supply chain. Ultimately, I believe that to build a reliable TVC between the two countries, we need mutual recognition between the U.S. CMMC and

Korea's K-CMMC. KRIT will support that path so that we can have smooth implementation, mutual recognition between K-CMMC and U.S. CMMC.

Lastly, I will talk about the plans to – for bilateral defense industrial cooperation in military semiconductor. KRIT is planning and implementing R&D projects on military semiconductor, including part development project, and will gradually expand R&D initiatives in semiconductor area, based on our related policies. And also, the KRIT has this project called Defense Industry Innovation Business 100 supporting five major areas, which includes semiconductor.

And the United States, of course, is a traditional powerhouse in system semiconductor design or engineering. And Korea is very strong in memory semiconductor. And it's also a manufacturer. I think cooperation with the two – of the two countries will result in great impact on the global market. And KRIT will actively support that path, so that we can have win-win situation, as the host of defense industry technology. Thank you so much. (Applause.)

Mr. Schaus: Well, as we just heard, there is a great deal to talk about in this issue set. And unfortunately, we are out of time for today's public discussion. So if I can offer a very brief summary of what I've heard, it's that there is a great deal, and increasing, alignment between the United States and Korea on the importance of supply chains, and the thinking about what we need to do to get to the next level. There is a growing interest and commitment to collaboration on S&T, on co-development, and downstream efforts from that.

And that there is, as a result of both of those, growing cooperation not just at the operational level – which I think we've been doing for 60 and 70 years – but at the industrial and the thinking level, which have been slower to catch up. And so that leaves me very optimistic that our alliance 3.0 is moving ahead and may soon hit a tipping point to an alliance 4.0, whatever that looks like.

But please help me say thank you to our presenters and our panelists. And that concludes this morning's session. (Applause.)

(END)