HOMELAND SECURITY EXPERTS GROUP (HSEG)

2021 HOMELAND SECURITY ENTERPRISE FORUM

PLENARY SESSION 10:

MODERNIZING HOMELAND SECURITY ENTERPRISE R&D

WITH KATHRYN COULTER MITCHELL, WENDY R. ANDERSON, EDDIE REDDICK AND CARA LAPOINTE, PHD

Salamander Resort

Middleburg, Virginia

Tuesday, September 14, 2021

Plenary Session 10:

Modernizing Homeland Security Enterprise R&D

UNIDENTIFIED SPEAKER: All right, our penultimate panel. We got one lightning round and one panel remaining, but here to take -- to talk to us about the modernizing the Homeland Security Enterprise Research and Development Program. As Dr. Charles Clancy, he's the Senior Vice President, General Manager at MITRE labs, but also MITRE's Chief Futurist. And I think we can all agree. Research and development across the enterprises is led from the bottom up at this point. We've heard talk about the need for a national industrial base policy, the need for a more cohesive R&D policy across DHS, but here to explore how we might actually put that into action. Leave it to Dr. Charles Clancy. Thank you.

MR. CLANCY: Great, thank you so much, and thanks all for sticking around. We're in the homestretch here. So, I'd like to start by just having each of our panelists give a quick self-introduction, and then we'll get underway.

MS. LaPOINTE: Great, thanks so much. I'm Cara LaPointe. I'm here from the Johns Hopkins Applied Physics Lab. And I'm co-director of something called the Johns Hopkins Institute for Assured Autonomy, where we make sure that all things that are AI-enabled work like they're supposed to.

MR. REDDICK: Yeah. My name is Eddie Reddick, Managing Director with Deloitte Consulting responsible for our work within several of the DHS components to include headquarters, as well as FEMA Secret Service, as well as CISA. And I have a…

MR. PRIETO: Terrific. Dan Prieto, Head of Cybersecurity Strategy for Google Cloud Public Sector, as well as a member of Homeland Security Experts Group. Before Google, I was director for Cybersecurity Policy on the National Security Council staff at the White House and also Chief Technology Officer in the DoD CIO's office.

MR. CLANCY: Great. Well, so I'm excited to have such a distinguished panel here to talk with us about this issue. So, a little bit of scene setting. Why are we talking about R&D right now? Well, lots of

reasons we're talking about R&D. But we're also in a very interesting moment in sort of bipartisan interest in increasing U.S. investment in R&D. And why are we in that position? Well, certainly China is a big reason for that. There's a lot of concern that China is outpacing us with their R&D investments. But we've also seen steady decline in U.S. federal investment in R&D as a nation. At sort of the peak of the Manhattan Project and Apollo program, we were seeing roughly 2 percent of U.S. GDP being invested in terms of federal R&D investment nationally. Now we're in a position where around 6/10s of 1 percent of GDP is being invested in terms of federal R&D. So, we've seen it in more than 1/3 what it was at its peak back in the 1950s and 60s.

Now, of course, industry has picked up their investment. Industries more than doubled their investment in R&D over that same period. And so, we've also seen this sort of natural shift to a much greater dependence on industrial innovation, combined with federal innovation, as we think about addressing the R&D needs of the U.S. government. But we have a new

administration, and just some of the numbers that have been talked about. The Biden campaign promised $300 billion in new R&D investment as part of their strategy. The White House infrastructure plan promised about a $0.5 trillion dollars in new R&D spending. And now, of course, we're watching the President's budget come together and be assessed on the hill. There's all kinds of other legislation floating around the Endless Frontiers Act notably that are investing in different aspects of this, want to see what actual numbers come out next fiscal year. But depending on how you count, this is anywhere from the potential for a 20 percent to as much as a 50 percent increase in U.S. investment in R&D, which is huge, particularly as DoD's R&D budgets are pretty much flat. I'm going to also note that DHS and T's (phonetic) budget is only about a 7 percent increase in the midst of all of this significant increase in federal R&D investment.

So, I would sort of posture. My thesis here is that we are kind of at the precipice of having the opportunity to fundamentally change how we as a nation innovate. We're talking about some of the largest

increase in federal R&D investment in a long time. And a lot of that, of course, has to do with how the U.S. can maintain its competitiveness on a global stage. But then the question is, well, how does the Homeland Security Enterprise fit into that? How can it effectively leverage those investments for its addressing its concerns and enabling its missions? So, I'd like to open it up to sort of each of the panelists to sort of reflect on that and talk a little bit about the opportunity they think this represents for the nation, and then more specifically for the Homeland Security Enterprise. Cara?

MS. LaPOINTE: Sure, you know, I think it's amazing that we're going to get increased investment. Right? But I think Claire said it really well before that, you know, we tend to throw money and people at a problem, and then we figure out the innovative solutions when that doesn't work alone. So, I'd say money is necessary to increase investment in these areas, but it alone is not sufficient. Right? We -- this is really an ecosystem promise, a human challenge. It's not a technical challenge to figure out R&D. We

live in a society that has thriving innovation, thriving innovation in the private sector, thriving innovation in the, you know, parts of the public sector, the labs, the FFRDCs, and UARCs, right? But we have to figure out those enablers to be able to harness that innovation, right?

We have heard about different acquisition, ways to do that about different authorities like other transactional authority, and how we can better leverage those, so that we can harness that. And one of the particular challenges is harnessing that innovation for those missions that are uniquely governmental, right, because that's what the financial incentives of this electronics commercial market we have are not going to drive. So I think that, you know, we have the power to do that. We just have to think about the whole ecosystem of the problem, and not rely on the fact that increase investment alone is going to solve this problem for us.

MR. CLANCY: Okay. Eddie?

MR. REDDICK: Yeah, I would agree with that. And it really comes down to I believe that technology

and the innovation aren't the real challenges. I think it's the people in the process. So, we've heard from several people, you know, today talking about whether it's acquisition, whether it's helping small businesses or organizations that have innovations that they want to get into the hands of the people that can use them. How do they do that? And until we, you know, take a hard look at those processes. And quite frankly, really, you know, figure them out for all technologies. If we look at emerging technologies that are no longer emerging, but in the past, things like cloud and other technologies like that. They were emerging, what 10, you know, maybe plus years ago. But the challenge with cloud in some of those technologies you looked at were things like the accreditation process. So, we went from DIACAP to DISCAP (phonetic) to RMF. And that slowed the adoption of a technology. And those same things still persist now. And they will continue to persist in the future, unless we take a hard look at the people and processes. And really, you know, say how could we make them pliable, maybe more flexible to be able to be ready to adopt those technologies that

come our way?

MR. PRIETO: You know, a couple of quick things. First of all, just as a disclaimer, my comments today are my own, reflect my background at my organizations. But, you know, personal opinions. I think I agree largely with what's been said before, and I want to sort of encapsulate some of what's been said. Eric Schmidt, Google's former CEO and Chair said, look, -- he was talking about DoD, but I think this applies to this conversation. He said, DoD doesn't have an innovation problem. It has an innovation adoption problem. Right? And this speaks to the people and process. Right? I agree that the reason that shift, you know, percentage of GDP, government share of R&D has declined is because venture capital firms, private firms have really picked up the slack at the bleeding edge of innovation, right? You think about cyber, everybody tends to think we need a lot of innovation in cyber. I looked in Crunchbase yesterday, there are 9600 cybersecurity firms listed in Crunchbase. There is no shortage of innovation at the technical level, right?

The problem is though, how do you get the innovation that is technical into pilots, into adoption, into operationalization, into regularization, and then into scale on government specific use cases. So, I think we need to marry technical innovation with innovation around operating models, innovation around process, the willingness to disrupt process. The reality with government is it's so much of process is people and paper driven. And so with that, I want to pick up the comment that cloud is in the rearview mirror. I don't agree with that. We've been talking about cloud since the cloud first policy, which was 10 years ago. Cloud adoption, as a percentage of spend, IT spend in the government is still sub 10 percent.

We are if you think baseball, that's first inning, second inning. And the reason there's that disconnect between cloud being an innovative technology platform and cloud being applied in a results oriented way, in a way that reduces toil that reduces inefficiency, is because we haven't translated these ideas into actually disrupting and changing business process. And I think, to some of the stuff we did on

COVID with a number of states, people suffered with contact tracing, PPE inventory management, you know, forecasting and modeling around COVID. The cloud lightweight applications and application program interfaces, data collection using cell phones, we were able to innovate that in a number of short weeks with a number of states without taking the heavy historic requirements, long cycle technology, build the process. So, the technology is there. And look, the cloud, to your point, is good at a couple things in a way that old technology was not scale, massive scale, speed, agility, security, and cost.

The reason that cloud adoption has lagged even though we've been talking about it for 10 years is because people -- it's such a huge cultural change. That's not the way I've ever done my IT. And because it wasn't -- it's not me doing it, I don't trust it. The 2018 Goldman Sachs survey that, about 60% of respondents said their big issue with moving to cloud was still this perception that it's not as secure as them building their own stuff. Right? I think that's shifting. We ran a survey, you know, just a couple of

weeks ago, 200 or so senior government IT leaders. And there is now about a 85% acceptance that you know what, the cloud can be more secure. And that speaks to a greater willingness, a greater openness to really partner with the government. But I look forward to talking more about this.

MR. CLANCY: So I agree that adoption, obviously, is a key challenge. I'll note that DHS and the Homeland Security Enterprise use cases though are not exactly the same as commercial use cases. Right? So, how does Do -- how does DHS presuming that at the end of the day, it's going to buy a commercial solution as a service for the actual deployed and operating system. How does it sort of swim upstream and influence the development of that technology so that it actually meets the requirements that doesn't even -- I mean, I think we have a challenge now where you try and write down all those requirements for the technologies fully baked, and you end up with sort of this chicken and egg problem. But how can we rethink that sort of the DHS approach to R&D that would shift towards being able to constructively influence the development of

commercial technologies, which is ultimately going to be a large part of what they end up buying at the end? And so maybe, Cara, you could -- certainly your background is in AI. I wonder if you have any thoughts on that specifically, from the AI perspective?

MS. LaPOINTE: Yeah, well, I think more generally, and not just from AI, you have to figure out ways to collaborate and incentivize, right? And you have to incentivize all different pieces of the ecosystem that we're talking about. Right? So the companies, you have to figure out ways to incentivize the companies. When you have emerging technologies that change very rapidly, and you have acquisition mechanisms that take a really long time to get things on contract, but we have to find new ways to do that, right? Commercial solutions, opportunities, type grants, their contracts and other things like that. But we also have to incentivize our own workforces. Right? You know, I think somebody said earlier, you know, we don't have a way to make sure our workforce is getting to yes, right?

So, we have to figure out ways to incentivize

our workforce, so that they can get to yes. And what are those mechanisms that we can then collaborate and bring together and say, hey, these are the specific problems that we have in this mission space, right? Are there consortia we can build, where you say we have this problem, and there's actual money behind it because you've reduced some of the barriers from the actual government piece of the government contracting piece. You put money behind it, and you bring different industries into one problem space, maybe it's through consortium mechanism. Maybe it's through another collaboration mechanism. But that's what we have to do is that we have to make this a shared problem as opposed to, I have a problem, I want you to solve it. We say we collectively have a problem. And we have the resources. I love the FWorks example before that I -- that somebody had where they literally were on the stage giving some money to small businesses, right? So, reduce the barriers, bring us together in a collaboration space, whether it's a consortia or other kind of space to solve shared problems.

MR. CLANCY: Okay. So, Eddie, I wonder you've got a lot of experience across various DHS components. DHS S&T, I think is a bit uneven and how it interconnects with those components, how it addresses those. Are there organizational things that could improve really the infrastructure inside DHS in the way that DHS S&T in particular, supports the different missions of the components?

MR. REDDICK: Yeah. I think there's been a lot of talk today about collaboration and how S&T partners with the components. And really having a conversation about the roles and responsibilities or even what Director Inglis talked about earlier like, really getting to a point of understanding, supporting and supported relationships between S&T and the components. I think that's really important. From the concept of what, you know, the term used is Homeland Security Enterprise, what is enter -- what's the definition of enterprise? What does that mean? And what is everybody's role in an enterprise to make sure that we get to the outcomes we want to get to?

For S&T, if I look at them, the challenge of

operating and working with different components, and in many situations, having conversation with the components individually, and then learning through those conversations that there are similarities across those components and being, you know, in a role of integrator. Well, how do we make that happen sooner? How do we, you know, bring in commercial organizations along for the ride, so that it's a conversation that people have upfront, as rather than one off conversations that don't necessarily provide the opportunity for the collaboration that you want, and the outcomes that you want to achieve.

And then if you do that, you have the opportunity to then, you know, better manage your spin, better manage your effort, your focus, and rather than spending time in one off fashion. So, I think the opportunity to bring people together and make it happen, you know, make it second nature and how the enterprise works together is important.

MR. CLANCY: So Dan, reflecting on some of your comments, I wonder, is the nature of dual use sort of changing? Sometimes I like to think of it as almost

the commercial application is that -- is really driving the market, right? And the secondary application is the government one. I wonder your thoughts on, is it time to start thinking about dual use technologies with sort of that flipped over?

MR. PRIETO: Let me back up a little bit from that question. I -- in a lot of the use cases we're talking about -- and again, just a quick comment is, is DHS thinks about its future? I mean, we're 20 years past sort of the start of the Global War on Terror. I want to step back a little bit in some of the mission areas where I think this innovation needs to occur. I think we've made the most innovation over the last 20 years on counterterrorism, full stop, because so much of the effort was focused on that. Right? I think, obviously, we need to focus on migration, on cyber, on bio, on climate. And when I think climate, I definitely think disaster response, emergency preparedness and response. What's interesting about all of those topics is that they're all complex systems problems, right? And the people and the resources and the technology that are applied to those need to help

address the complexity of those systemic problems. Right?

So, I want to link to the comment earlier about incentives. In general, I think we have to change the discussion around AI people like, Oh, we fear AI. AI is going to take our jobs. I think when you're dealing with knowledge workers, which are what analysts and people in government are, it is not going to take people's jobs. In fact, it is going to make you radically more efficient and effective at what you do. Right? So, by taking toil out of a really difficult or complicated or paper based process, the incentive for people to work with the technology isn't that it's going to replace you nor is it a black box, it's going to make ethical decisions for you. It removes toil, right?

Take the example of cyber, the amount of cyber telemetry in your average organization is doubling every year, every couple of years. We implemented a cyber-analytic platform. Google did for New York City Cyber Command. They are ingesting 20 billion log events per day from several 100,000 users of the city,

several 100,000 endpoints. There's no way you can ever solve that by throwing more people at it. So, for all the discussion about hiring more people, you also have to think about ten-axing (phonetic) the productivity of the people you have and hire. Right? That's the way you incentivize them because say, look, you're never going to solve this just by more hands on work. You have to be way better at what you do.

In terms of how you incentivize the private sector, when thinking about complex systemic problems, I think director Inglis got to this the other day, it is still not sufficiently clear to private sector actors on cyber, for example, what government is going to do to help them. Yes, they get information bulletins. Yes, there's some more investment dollars we can provide. Yes, we send out information on patches. But if you break any cyber-attack into a framework that -- under the Obama administration, we promulgated with presidential policy directive on incident response, you can think about response to any attack and protection as dealing with the threat actor, who is the bad guy. The asset itself, which is

basically what's the vulnerability. And then, what we call the business response. How do I communicate to people if the data has been lost? How do I protect people from identity theft after there's a big data breach?

The way we focused on cyber to date is by telling the private sector to cover down on your vulnerabilities. We have not made a sufficient enough for offer to them to explain to them how we are going to systematically deal with the threat actors. And it can't just be prosecutions or the idea that we're -- if someone pings us on cyber, we're going to take out something of theirs. It has to be, for example, in the United States, if nation state actors are spinning up, attack infrastructure, command control infrastructure, what is the government going to do far left of boom well before a private sector actor has to worry about protecting their own patch, right? And this starts getting to your conversation about use cases.

So the use cases to me, of course, the technology is dual use, commercial application, government application. But equally important or more

so than dual use government scenario versus commercial is a clear delineation of roles and responsibilities and a clear offer from government on what they are going to do to solve the systemic problems on these complex system issues, because so much of the systemic problem stems from the fact that this organization -- this country is organized in a highly pluralistic way. Things are fragmented. And by design, our constitution was built that way. But that means back to the industrial policy question. We're not good at having content -- sorry, effort that is coordinated and collaborated because there are so many seams between civil and military, public and private, domestic and international. Those are the seams that adversaries -- or not even adversaries, hurricanes take advantage of, right?

MS. LaPOINTE: If I can jump in on the systems engineering point for a second, it's sure this is a very complex system of systems engineering problem. But even more complex is that we're talking about digital technologies, which need a different approach to systems engineering than our more traditional

hardware technologies. A lot of our government systems engineering's processes are focused on hardware. But we have software. At its essence, these -- a lot of these emerging technologies are digital and their software. And we need completely different ways of looking at it. For example, if you think about kind of acquisition versus sustainment, we often think of, you know, the biggest cost is when you first get something in and then you establish it, you develop, you deploy it, and then you just have to sustain it. But when you talk about digital technologies, and this is where AI has a completely different model, you have to bring the idea of research and development into your operation sustainment phase. That is a completely different mindset that we have not approached yet. And these are the kinds of fundamental organizational and policy and process challenges that we have to get over if we're going to actually realize the benefit of emerging technologies.

MR. CLANCY: And I think from a systems engineering perspective, a very interesting part of that is test and evaluation, right? And I know

certainly a lot of these digital technologies, we don't have good ways to do test and evaluation. Certainly in the cyber domain, it gets to checklists that get you different certification levels in the cloud. But in some of these other emerging areas like AI, right, where if you have a system that's been certified, but then it's able to learn new things in operation, right, how do you continue to test and evaluate and certify it? Let's see. So, I wanted to give an example of a use case based innovation approach that I think is working reasonably well. And it comes from DoD, where they have spent, I guess, Phase I, it was -- it's the 5G based pilots that DoD has been doing.

I think there's an interesting example and something -- it might be something constructive, we could use as a discussion point for how DHS might think about some of its larger scale investments. But essentially, DoD wanted to have all kinds of cool IoT use cases that would have a military value. And really, not so much acquire these and deploy them at bases around the country, but really create an environment where vendors could come together and be

incentivized through OTA consortia and funded to figure out how to get all their different pieces working together, build the relationships among the vendors, so that at the other end of this, there would be a shrink wrapped commercial product that DoD could ultimately go off and buy, to use for 5G for a wide range of different use cases.

And so of course, it wasn't cheap. We -- the Phase I was, I think $600 million. There's another phase that's about to start. So, it's pretty significant investment. But not only has it really catalyzed the domestic telecom ecosystem around 5G, the needs that DoD has, it's also really helped energize a domestic 5G vendor ecosystem in the first place, right, because we had lost much of our expertise in that domain to China, well, lost our ground to China as U.S. companies merged with European counterparts over the last 20 years. So, I find it a sort of a fascinating example of where I think the dual use coin really has flipped, right? DoD is investing in these 5G pilots, primarily because they're going to lead to economic competitiveness to the U.S.

And as a result of being able to sort of shape the focus to these different use cases, there will be the opportunity for DoD to kind of buy a service from the vendor ecosystem that matures to this process. Right? So, I think that this is kind of a really interesting model, where I think other agencies should look at trying to inject their requirements into prototyping, experimentation and pilot sorts of activities. And I wonder if any of the panelists have ideas in other emerging technology areas where that model might work, particularly for DHS mission areas.

MS. LaPOINTE: So also, I'm a huge proponent of the consortium model, right, for a lot of reasons. One, because these technologies move very fast. We need different ways of approaching these from a community based perspective. We need collaboration, right? And by using a consortium -- I came out of the DoD world on the acquisition side and the Navy. And, you know, if you were to go out to a vendor and say, Hey, I need help just writing the statement of work for what I'm doing, because I am not as smart as the vendor base right now, in terms of how we're going to talk

about and how we want to acquire this technology. You couldn't do that, right, because of our acquisition regulations and federal regulations and laws. But if you have a consortium -- the beauty of a consortium in some ways is you have symmetric access and symmetric information. So, you can go out and to your whole kind of group of industry partners in a consortium and say, hey, let's figure out a way to make the government smarter on this technical issue, so that the government can be smarter when we write our RFPs when we do this process, right? Because the government -- no sector alone has the full capability, capacity and agency to implement emerging technologies, right? And so, when you can find innovative ways that you bring industry in, you bring government in, you bring academia in, and you can pull that knowledge, it's the only way we're going to be able to collectively go farther faster together.

MR. CLANCY: Okay. Eddie, any thoughts?

MR. REDDICK: Yeah. So, you talked about some of these use cases and you mentioned 5G. And so, our firm has been involved with one with the Navy around

smart warehousing. And that smart warehousing effort leverages 5G technology to, you know, connect systems such as your asset management system, your inventory control systems, potentially wearables from the individual, as well those biometrics, so that you can have situational awareness on all things that are happening in that warehouse. And that's technology that's being leveraged on the commercial side.

And when we talk about dual use, I mean, much of the business of the government is also the business of the commercial side, financial management systems, inventory control, supply chain systems, even cyber, those are the same challenges that our commercial counterparts are dealing with. And they have invested in those systems and they can be brought over, because we use SAP, they use SAP. They're leveraging, you know, some of the same technologies and pulling them together for a, you know, a whole, you know, in a broader solution. So, those are available and can be replicated because the processes and the outcomes are the same, regardless of whether you're commercial or you're working on the government side.

MR. PRIETO: You know, thinking through that, where these consortium models might work or where it would make sense for groups to get together to think about requirements that are more business outcome oriented as opposed to inputs oriented, which is too often the case I think on a lot of procurements. I think there's a couple areas I think of. One is the Internet of Things, and the increased sort of, you know, risk to an automation of industrial control systems, right? These undergird our critical infrastructure. This is a new realm for cyber. Yes, we've been talking about it for many years, but the IoT surge is coming. And we know, nation, state adversaries are very much targeting our critical infrastructure, so the risk is going up. And historically, our security focus has been on information technology systems, and not enough on operating technologies to control operating systems.

Second area is around supply chain. Supply chains, you know, are I think among the poster children for complex global systems that are flooded with tons of data. But the challenge is, how do you make sense

of the data at scale because the data volumes are so big? And how do you connect data together because it can be so fragmented? So, in the areas I'm thinking are important are much better real time visibility into the supply chains, where our points of risk, where our point of interconnection, where our points of potential cascading failure that you wouldn't notice, if you were looking just at sequentially different parts of the supply chain. I think there are scale issues on the inspection side in terms of inspecting, whether a hardware in your supply chain may have been tampered with or be fraudulent.

Same thing on code. We saw this with solar winds. So many things come into the enterprise. And because they came from a trusted third party, and that third party code was signed, we presume it's okay. But there's not enough. And this is difficult to do. How do you inspect those things? And you don't necessarily have a signature of a bad section of code. It's, how are they behaving? Is this version of software? You know, this version of solar winds versus that version of solar winds? It's doing five new things. And it's

never done these five things before. Why is it trying to access an administrator control point? Why is it trying to access a financial database, for example.

The other area, the third area that I thought of in terms of innovation, again, very data driven, very complex, but we need much better foresight and insight is on modeling and mapping around fire, around flood, around hurricane, right? Those groups, particularly, weather, I mean, there is an interdisciplinary core, working through FEMA, working through governors that knows how to deal with hurricanes, but there are large parts of the country that don't have the muscle memory because they're not used to getting hit by hurricanes. You have large parts of the country that aren't used to having drought conditions or fire conditions. So, you need to arm people with more data, visualization of that data and the ability to have more foresight and predict, again, fire, flood, hurricane and all that. Like, again, complex, large scales systems oriented data that, you know, I think the technology can give any user a much greater ability to make sense of it, and can actually

democratize the access to those kinds of analytics.

MR. CLANCY: So, I think we've had a lot of examples here of sort of engineering and technology related innovation. But we just had a great panel on civics. And I'm curious, should DHS be investing in research and development in the social sciences beyond kind of the hard tech spaces?

MS. LaPOINTE: Absolutely. All right, you know, I work on Assured Autonomy, right, which is making AI and autonomous systems work. And I'm an autonomous systems engineer. But I always include people in the system, right? It's really the intersection between technology and humanity. That's important. It's those intersection lines. And if you don't have social scientists at the table, you are never going to solve the problems that you want to solve. If you just bring technologists to solve a problem that is fundamentally a human challenge, you won't ever get there.

MR. CLANCY: Any other thoughts?

MR. REDDICK: Yeah. I am not a social science scientist. But I would say, yes, the intersection of

people in technology is very important. I think the idea of understanding the impact of people as you roll out that technology, how people receive that technology. You talk about AI. you know, in one of the sessions earlier, we talked about how you can use AI to, you know, basically identify potentially fraud, maybe in somebody in FEMA who is making false claims. There's also the opportunity potentially to leverage that AI to let people know in that same area who haven't made claim to who don't know that they have money that's available to them.

And maybe the opportunity is to say, Hey, your neighbor has filed a claim and you don't -- you have it, why not? Do you know this money is available to you and use it as a positive? And so it's not just, you know, find the bad guy, identify the bad actor. It's also along with some sort of stakeholder or outreach effort to let people know that this technology found you. And that's why I'm reaching out to you because you're missing an opportunity to take advantage of something that's available to you. And I think that's important.

MR. PRIETO: You know, I'm glad you brought this up because I think it is absolutely fundamental that we also invest in the social sciences on the R&D side. And for the following reasons, we have one nation state adversary that is actively trying to corrode and undermine our civil society, full stop, right? We have another nation state adversary that is seeking to gain advantage on the economic front through a close coordination of national industrial policy, and also leaping ahead through intellectual property theft. Both of those things have to do with liberal, capitalist democratic society, right? Those aren't science things.

And the things that analytics and AI anal can help with around sentiment analysis, assessing, you know, the confidence and trust that people have in their institutions, and being able to detect the information environment, to see where -- look over the horizon in terms of where government organizations need to be more active in countering either misinformation or disinformation or where they need to be more proactive to just try to help rebuild confidence. And

this gets back to Suzanne's excellent panel on civics. But I think it goes without saying, particularly given what we know, our nation state adversaries are doing, we need to invest in the social science side as well.

MR. CLANCY: All right. Well, with that, let's transition to questions from the audience. Any -- anybody brave enough to ask a question? Now, I spent a decade as a professor, so I'm going to use the Socratic method here soon. All right.

UNIDENTIFIED SPEAKER: So talk to us, if you will, about the need for a Homeland Security Enterprise, not just department, strategy to address R&D going forward. Do we need one? Or do we continue with this sort of haphazard, organic R&D efforts?

MR. PRIETO: Any -- so I'll -- I guess, we're seeing a lot more interest in national strategies, right? OSTP is leading the charge now on a whole range of an emerging technology areas. And I guess, as that translates down to the Homeland Security Enterprise, thoughts on how that ecosystem could be more coordinated in its own strategies that integrate across really, beyond just whole of government, but only whole

of nation and I think is critical.

MS. LaPOINTE: So, there was an interesting discussion in one of the earlier panels today about the idea of kind of control -- coordinating and controlling at the highest level in terms of what we're doing versus harnessing, right? I think there is value in having a strategy. But I think we need to be careful to not try to kind of control what we're doing. And more, it's a strategy for how we harness what's out there and focus that innovation energy on some of our unique mission areas.

MR. REDDICK: Yeah, I think there is a need for a strategy. But I think that strategy should be about to what you're saying, the opportunity to bring people together to recognize that you have similar needs. And so that you aren't, again operating in silos. So, the strategy should be in -- and again, if we are really talking about a term of enterprise, it is bringing everyone together so that they can hear that, hey, we have the same need or we're asking the same questions, so that we don't have to have one off solutions. And if it is truly a system of systems, you

need to have everybody at the table so that they understand what's happening to the left and to the right of them, rather than just what's happening for me.

MR. PRIETO: Yeah, I agree with all those comments. I think the power of the government to convene, and then once it convenes, sort of serve in the quarterback role. I think also, and we've talked about this in several sessions, the government making more clear what it is bringing to the table as opposed to telling other people what they need to do better because we've been doing that, like for as an example on cyber for a long time. It needs to be clear what they are going to take on in terms of countering the threat, whether it's overseas or here. I think the other piece of government is it thinks about the enterprise needs to communicate more clearly to the private sector is how the government will improve the fragmentation of the government itself, right?

Okay, let's talk about cyber for a second. When does the FBI help me versus DHS? There's this new policy called "defend forward." It's not going to make

me confident that you're actually better at telling me about the threats that are coming my way, if I agree with you that my job is to protect my patch on the vulnerability side. However, I also think I can't be told to just do better and fend for myself against nation states. Fine, if it's criminals or fraud. Fine, I accept that responsibility. But it is the government's responsibility to protect the nation against nation states, right? So a clearer, more directed set of convenings on complex problems. Again, this notion of quarterbacking is key, but then also a clear statement about what the government will do and how the government will operate more seamlessly.

MS. LaPOINTE: And if I can just jump in on one of Eddie's points in terms of bringing everybody to the table and breaking through silos. That's really important, and then you have to think hard about who all those people you have to bring to the table are. It's not just the technologists and the end users, right? It's also the social scientists, the domain experts. It's also the folks involved in all these processes and policies, right, so that we can bring

everybody together and figure out a solution. Because you may figure out something that works really well for technologists, but then we don't actually have the test and evaluation methodologies, or we don't have the other process elements in place. So you have to really be diverse when you're bringing folks to the table to come up with that strategy if that R&D strategy is actually going to be helpful.

MR. CLANCY: Yeah. Any other questions? Yeah. We've got one back here.

MR. BOSWELL: Teri Li Hoffman-Boswell from MITRE. So, I just like to pull the thread on that notion with regards to the roles and the role of government. When it's a nation state actor versus the role of industry, if it's some other bad actor, how would you know in the moment?

MR. PRIETO: I think there's been a lot of talk historically about attribution, right? I think you prepare for situations, regardless of who the threat actor is. Again, I think it is incumbent on the private sector to cover down on vulnerabilities and patch and run training programs and make sure their

board is aware of cyber, regardless of who the bad actor is. At the same time, they don't have frequently visibility further left of boom on what's happening. They don't necessarily see all the classified intelligence on what our adversaries are doing. They don't necessarily see those actors. You know, in the U.S., sort of stealing IP or creating command and control infrastructure on commercial networks and infrastructure, that's up to government.

So, I don't think you have to pre solve or think about every incident, thinking you can't do anything. I think the question presumes that you're waiting to do something until something is actually blown up. Before that, there is a lot more that can happen in terms of government being more open on the information sharing side about the threat, because a lot of companies don't have the wherewithal to see into nation state threat. I think, again, the "defend forward" strategy, which DoD and DHS are collaborating with, which is you really look -- you don't tolerate penetrations by nation states into critical infrastructure, and just call it out to espionage if it

happens. And therefore, again, I don't think you have to pre solve, knowing which actor is which. I think you just have to do a better job describing the systemic problems, knowing what the motivations and incentives and, you know, activities of our adversaries are. But I appreciate any other thoughts from you guys. Okay.

MR. CLANCY: All right. Well, I think it's been a great discussion. This panel, of course, built I think on a lot of the discussion we had in the breakout workshop on emerging technology earlier for those that attended that. So, it's a great to hear a kind of some common themes between the two. It sounds like we need a lot more consortia that are really looking at partnering for research and development rather than traditional requirements driven acquisition for a lot of these new areas. And I think that's a great direction that can leverage all of the innovation that's happening more broadly in industry, towards the Homeland Security Enterprise. So, join me in thanking the panel.

* * * * *