Frank Konkel:

I'm Frank Konkel, Executive Editor at Nextgov. And thanks for closing out our two-day cyber summit, the Gov Exec Cyber Summit. We appreciate your attendance. With me today, Laura Galante, the Intelligence Community Cyber Executive and Director of the Cyber Threat Intelligence Integration Center, CTIIC.

Laura Galante:

Got it.

Frank Konkel:

Laura, tell us a little bit about yourself and your role and we'll get started.

Laura Galante:

Sure, yeah. Well, congratulations to the survivors. I know we are the very end of the day here, but excited to be with you. Look, I come out of the private sector into this role. I had done quite a bit of work at Mandiant, FireEye Mandiant, over time on the intelligence side of the house there and was the Director of Global Intelligence when I left in 2017. And then spent the next five years, had my own company, did a lot of work in Ukraine on that first US aid money that went in on improving Ukraine's cyber posture. So a lot of stories from that side, but not for today. I came into this role, the director of CTIIC, as you mentioned and the IC Cyber Executive about a year ago. And do you want me to jump into?

Frank Konkel:

Sure, yeah.

Laura Galante:

A little story on kind of where CTIIC came from and where we are today?

Frank Konkel:

Started in 2015.

Laura Galante:

Okay.

Frank Konkel:

And we've come a long way.

Laura Galante:

We have.

Frank Konkel:

Let's talk about it.

Laura Galante:

All right. We'll first, actually, start back in late 2014. Does anyone remember the Sony attack? Okay, good. All right, lots of nods in the room. All right. So the quick version of it is.

Frank Konkel:

The one we made a movie about.

Laura Galante:

The terrible Seth Rogan movie. So it's just about Christmas 2014, parody, very clearly a parody to the US audience, comes out about North Korean leader. And North Korea does not see this as a parody. They see this as a true kind of existential threat on North Korea. And they go after Sony to the point from a network attack standpoint that Sony is down to the ground. They have to go down to the basement and pull up the old credit card machines to go and do transactions for lunch. I mean, Sony employees are truly kind of dead in the water from an ability to operate standpoint because of this network attack. And in the government at that time, the USG and the IC looks at this incident and says, "Wow, this is really a debilitating cyber attack. How do we put together attribution behind this?"

"How do we have a single common operating picture that we can look at?" Worked with the private sector who's out doing incident response, happened to be in Bandian at the time, and then put that picture together and say, what do we do about it? What are the policy responses? What do we need to put in action here? And CTIIC is born out of the experience of needing to improve developing that common operating picture. So CTIIC gets charged with, in February, 2015, standing up to integrate intelligence across the IC and across the private sector, to build a single conclusion to what the US government knows about a cyber incident. So I'll stop there. That's kind of the short history.

Frank Konkel:

Well, so that's how it started. What are the main priorities right now for CTIIC and where are we at compared to 2015?

Laura Galante:

Yeah, great. So 2015 feels like 20 years ago for anyone in this space I'm sure. And it certainly has shown with CTIIC, it's gone a long way in those eight years. So today when you look at OD and I, which is where CTIIC is, the Office of the Director of National Intelligence, CTIIC now has the policy support function. So kind of the last mile of intelligence support and intelligence production for policy needs for the National Security Council, for the Office of the National Cyber Director and other policy customers that lives under the National Intelligence Manager for cyber who reports into me and CTIIC. And then the other side of the house that we have is that more traditional analytic integration function that I outlined in the 2015 start of CTIIC.

So putting together that single picture with the intelligence that we have. The third pillar that we have is around investment in collection, synchronization and unification across the IC. No one here, no one watching online would be surprised to know that there's a lot of different pockets of money invested across the cyber intelligence landscape. But finding ways to uplift that, see where our gaps are, see what the buy versus build calculation is in different spaces, really important. And something we're charged with at OD and I, so those are the three columns that I've got within the CTIIC of 2023.

Frank Konkel:

And the engagement factor, how much engagement are you seeing from industry out there and agency partners as well?

Laura Galante:

I mean just to think of the commercial cyber threat intelligence space here over the last 10, 15 years is to see a sort of sub-industry emerge in a market mature and a capability really arrive. And when I think back to the early days, coming myself out of DIA and going into Mandiant in 2012, I remember getting the call to come to Mandiant and they said, "Hey, we've got this data to look at from an IR work, from instant response that we're doing. We heard you look at data and make sense of it."

Just the concept of like we're building an intelligence team in the private sector around this was still that new just 10, 11 years ago. And here we are today with, I can't even estimate how many different cyber intelligence products and companies out in the landscape here. So one of the things on the other side within the IC that we've got to do is be able to look across that proliferation of different cyber intelligence providers and make some sense of how do we buy this in a way that's effective for all the different 18 IC agencies that are out there? And then how do we solve for the specific use cases that CIA will have, that FBI will have, that DIA would have, and then figure out that layer and around tailoring the approach. That's just the commercial side though. Yeah, go ahead.

Frank Konkel:

On that same note, what can industry do better? I mean it's a big landscape now. How do they differentiate for you guys?

Laura Galante:

Yeah, so I think the place, and maybe we'll get into this a little bit when we talk about threat as well, but the place where there's a real opportunity from the industry side and a real need from the government side to me is on how we understand technologies that are being built outside of the US and the vulnerabilities inherent in those technologies is somewhere where we've had a lot less visibility traditionally in the US intelligence market. In commercial intelligence market. I'll give you an example. For the last 20,30 years, US techs really been dominant obviously in the types of IT enterprise ICS systems.

Most of the tech that business runs on has frequently been from US companies that's given the US from an intelligence standpoint, inability to understand the threat in a much more synchronized way. When you look at how you look at Alibaba, when you look at name your prominent tech firm in China, the user bases of these companies have tripled, quadrupled or more just in the last few years alone. And they're not just in China, they're global. So the more we can get a better understanding from an intelligence standpoint about how those products are working, what user bases look like, that's a place where I think understanding those vulnerabilities and the threats that different technologies pose outside of the US is a place where we've got to stay focused.

Frank Konkel:

So on the threats, you teed it up great for me, but we talk about China as a major threat. You have expertise in Eastern European issues as well though. And we have a conflict still going on with Russia and Ukraine and Russia's up and singled out as a big challenge and threat actor for us. How is the IC keeping pace with those threats at the moment?

Laura Galante:

So without going into a deep threat landscape piece here, I'll pull out a couple highlights that I see from some of the actors that you mentioned here, Frank. So when we're thinking about the PRC, thinking about the threat to telecom is really key here. And I'm hard pressed to even define the telecom sector at this point because it goes from everything from undersea cables to cloud and everything in between. Different network layers, I mean, that entire ecosystem is something where we've seen China, in addition to Russia, have a real focus on exploiting for intelligence collection, for disruptive opportunities and more, and influence operations as well. So being able to understand the threat at different layers within that larger telco and ICT space, really critical, because we see the adversary there. On the North Koreans and on the DPRK, I think it's again no surprise that the crypto piece here is really the focus of how we're seeing that threat.

Frank Konkel:

It is amazing how that has changed, I mean, how much money they've been able to get through crypto as well.

Laura Galante:

Really unreal.

Frank Konkel:

It's like a lot of their operations.

Laura Galante:

And you know, you think about this, if it was happening in real worlds at banks and someone's walking in and taking the sums of money that are out there.

Frank Konkel:

30 billion dollars here. Yeah, it's insane.

Laura Galante:

625 million in one hack alone last year. That would be the story of every day of the week, right? So we've really got to stay focused on the level of innovation and agility that the North Korean hackers have on the side. You can think back to 2016 with the bank hacks on SWIFT systems that were going on. And today you're looking at an even more sort of ingenious ability to go after the crypto system in really specific ways.

Frank Konkel:

So we've got our new cyber strategy from the Biden administration that came out, long awaited. How does OD and I fit into that and the intelligence committee at large? What's the responsibility and roles there for you guys?

Laura Galante:

Yeah, great. So I think one of the kind of notable pieces in there is around disrupting and dismantling threat actors. No surprise, the IC has a play there. And some of the implementation that will go into making the strategy real will be very public. So one of the pieces that OD and I is leading on is removing the barriers from commercial intelligence coming into the IC and then also being able to push good intelligence out. So that's the piece where we've got to lead and we're really synchronizing the ICs efforts there.

Frank Konkel:

Lot of discussion today on artificial intelligence. It's really kind of everywhere in the news now. I'm curious about your broad thoughts on that subject, that technology as it relates to the IC. There's no shortage of potential use cases for AI. It's already seemed to have a huge impact on even the pop culture discussion. I mean news networks now are running full hour long programming on just this subject. And I find it fascinating. Some of it seems a bit weird to me and cause for concern, but there's also a lot of good potential there. What are your thoughts?

Laura Galante:

Certainly the duality of it's really interesting. If I had a nickel for every time someone in tech or in the IC has said, "We've been doing AI for the last 20 years," and then goes to opine on the last four or five months, I would be up there with the same kind of dividends the North Koreans have on crypto. But look, the sort of thought process here that we've got on the IC side is we're looking at a commercialization, an availability, especially with the large language models and with generative AI in just the last four, five, six months that's really a game changer in how actors will use it. And what we also know is we're not going to be able to develop norms, figure out privacy controls standardization quickly enough to mitigate what are going to be the risks and threats that these posts. That's just the reality of how fast this is moving.

So what I think the larger community can do, and there's no shortage of AI ethicists that have been out there and futurists who've been thinking about this for 10, 15 years. I really challenge them to start thinking about how do you consider guardrails in this space? And it's going to be people who are really close to the models, who are really close to the different use cases, who are watching the creativity in this space, who I think are going to be closest to the edge to come up with solutions that will outlast this initial kind of burst of activity that we're going to see.

Frank Konkel:

Or do you think the government is nimble enough to bring in AI at a pace that commercial industry will be able to? Or do you think because of our step back, look at the procurement system, we're not necessarily geared to do that? Or how do you think the government can handle that challenge?

Laura Galante:

I mean I think when you think about agility in this space and adopting and continuing to adopt AI, it's not like we haven't been, right? But we have to position ourselves so that we can see what commercial solutions are going to be a better model to buy versus build ourselves. And that by build calculation is something that's really dynamic right now and how the IC is looking at technology acquisition. So I think of agility really broadly here because I think we've got to get to that place in our acquisition mindset to make those calculations, to adopt what's best.

Frank Konkel:

And a desire for the IC to bring in more commercialized startup new technology to its ranks. I mean that's something that we're looking to do better. I mean, aside from what we just talked about, are there other ways that if I'm a startup company that I can get in contact with you and say, this is what I think I have to offer. How do I do this? I'm not a normal government player, what do I do?

Laura Galante:

Yeah, we're working. I mean it might not be me as the best athlete on exactly that question, but when we look at the IC and you look at some of the agencies that we have here, I'll name NSA's Cyber Collaboration Center as one place here. Where are there innovative partnerships that we need to have? And we have people either developing a technology or they have a really specific data set. I would encourage those folks to find the right door within the community to knock on and say, hey, this is something and here's how we're collecting it, here's how this data works, what have you.

And I think we're getting better collectively in the IC that no matter which door you do knock on, whether it's NSAs, whether it's another agency, whether it's through CISA JCDC, when it comes to cyber, that door or window open will still lead into finding the right use case for that tool, for that conversation. It doesn't have to directly be a technology. It could also be, hey, here's what our salespeople are seeing in China right now. And this might be a really interesting piece for some trade negotiations or whatever that use case might be. But we're getting better at integrating those inputs, whatever they look like, into the IC.

Frank Konkel:

So aside from the tech, I mean workforce issues were talked about I think a couple panels ago. I think they're one that can get overlooked when we were talking about technology, but how is the IC dealing with its workforce challenges? I always think of the IC as kind of a unique, cool place to work. Maybe I haven't been in DC too long as a Midwest kid, but it always seems like a cooler place to market yourself. I'd rather say I'm with the CIA than maybe transportation department.

Laura Galante:

Poor transportation.

Frank Konkel:

Yeah. But how are you dealing with that challenge? Because it's a big one. I mean, even leading industry companies are having a tough time keeping, recruiting and retaining talent in these ranks.

Laura Galante:

The way that I think about this, I know workforce was covered really well in that panel, to your point, is that we've got to consider that inherent value proposition that you're getting at, which is the ability to serve. And also when you think of it from just the really cool standpoint of what you get to do every day, nobody's got the authorities that the USIC has out on the private side commercially. Just the ability to not just use the different intelligence sources and data that we have, but also the ability to push forward on the mission against adversaries. And Russia, Ukraine over the last year plus. But I see some folks out there who've been on the front lines of this for far longer and remember the 2014 invasion really vividly here, that's a call to duty that's really clear on the outside.

And I think the IC can capitalize on that sense from people. Let me throw one more thing in, because it came up this morning at my cyber strategy board that I lead with the IC and I thought it was a kind of neat point. I invited the State Department, their Bureau for Cyber and Digital Policy over this morning. And one of the big pieces that they shared with us is how often they get questions around what the US is doing on cyber workforce from other countries. Not that we've got this figured out at all based on how many panels are on it today, but this is a global problem. It's not even just the ICs, it's not even just a US issue. We've got to find a new paradigm here to think about how we look at talent and think about the time it spends in this space.

Frank Konkel:

And just on that note, desired talents and skill sets that you're seeking at CTIIC. What types of roles are you looking to fill and bringing in and meet that mission?

Laura Galante:

I love creative thinkers who can go outside the box on how we challenge threats. So there's a very traditional sort of InfoSec mindset that a lot of folks grew up in in the cyber world on how you unpack and look at threats from a digital forensic standpoint. And then there was increasingly sort of strategic analyst type role that came in of how do we look at country's goals and marry those up to adversary activity. But I think the next place that would be really neat for us to start driving on, especially with the continued focus on AI and the threat it poses and the opportunity we have with it, is people who can start to think about the application of these newer technologies, of these new more iterative ways to process data and what types of data sets could be pulled in to start answering really hard questions on the threats that are we're facing today.

Frank Konkel:

We have another minute or two if there's any audience questions, raise your hand. I'll be happy to take them. Otherwise that kind of concludes mine. We have one question over here, one question over here. Let's get those two and then we'll wrap up.

Speaker 5:

We had a question earlier that some of us were asking about that John Sherman, the DOD CIO talked about the fungibility of talent in and out of the government. And one of the questions I wanted to ask of the other panel is what's being done so that people can actually leave OD and I come back into OD and I? It just seems like the model is still the same. You leave, you have to get cleared and you have to come back. You've made the transition. What's the community thinking about in terms of letting people go and come back? Because I think there's real value in bringing people back. Thank you.

Laura Galante:

You're right on that. And this is one of D and I's priorities. It's something we've been working within OD and I itself to find the right model here, whether it's highly qualified experts, whether it's different fellowships, but finding some more flexible, fungible is a good John Sherman word there.

Speaker 3:

There's cyber pay policy out, Title Six that's actually part of the core capability. Title Six is allowing people to leave and come back and not get penalized in federal points. But it is around specific cyber professions.

Laura Galante:

And there's continued work on that in addition to other areas where we can bring in the expertise too for a specific question or a specific set of workshops. Some of this doesn't have to be the full-time employment model. It can also be bringing in that expertise in pockets at the right time in place.

Frank Konkel:

One question over here, the gentleman who had his hand up there.

Speaker 4:

I don't know if it's a question or not, but I'd like to commend you on what you did in Ukraine because the Russians had to go to kinetic devices to attack the power grid over in Ukraine and then that speaks quite highly. Because as you know, they tried to attack that first. So congratulations on the work you did there.

Laura Galante:

Yeah. So questions around Russian attacks on the power grid. The mic was a little tough to hear, but there's so many different dimensions in the war in Ukraine right now to talk about on cyber. It's worth its own panel another time, of course. But one thing I will say to this point is the more the Russian forces are degraded from a conventional warfare standpoint, and they certainly have, there's public estimates around a hundred thousand dead on the Russian side on this now. But the more that the Russian military is degraded over time, the more they're going to have to look to capabilities like cyber and space as a way to have a continued force going forward. So even though I think cyber's played out a little differently than some folks have thought over the course of the last year, year and a half now almost, I think that the dynamic here is going to continue to change as Russia has to make harder and different choices over time.

Frank Konkel:

Was there one more question really quickly right here? And then we'll get you all out of here.

Speaker 6:

Yeah, my question's regarding the cyber coin and Bitcoin and all that regarding North Korea. So the beauty of the tool is that you're able to track all the transactions that are made. So from that standpoint, why aren't we able to take the money back from North Korea that they've stolen through the use of these tools, Bitcoin and so forth?

Laura Galante:

The questions around traceability of cryptocurrency transactions, from the North Koreans in this case, but the ecosystem that these different attacks are happening in is really wide. And the traceability and the level of mixers involved in changing the coin before it gets to FIAT, really complex here. And this is why you've seen sanctioning activity around the mixers here in the last year as well from treasury side of the house. So without getting into too much more, just the complexity of how the North Koreans have been able to cover their tracks, if you will, in this space really continues to evolve. And it's something where we're stuck in a little bit of a collective whack-a-mole and trying to figure out the right places to squeeze in the crypto ecosystem to make that harder to do.

Frank Konkel:

And Justice Department has come down hard on some of these too, indictments and stuff. That wraps it up. Laura, thank you so much for-

Laura Galante:

Thank you.

Frank Konkel:

...making time. I appreciate it. Special thanks to our underwriters for their support in this summit and for all of our attendees, whether in person or virtual. All the sessions from yesterday and today will be up on website for on-demand viewing. So you can rewatch if you need or share if you need. And that will wrap it up. Hope you guys have a good rest of your afternoons.