

Center for Strategic and International Studies

TRANSCRIPT
Online Event

“Sparking a Revolution in Open Source Intelligence”

DATE
Friday, December 3, 2021, at 2:00 p.m. ET

FEATURING
Robert Cardillo
President, The Cardillo Group; Former Director of the National Geospatial-Intelligence Agency

Sean P. Roche
Director of National Security, Amazon Web Services (AWS) International Public Sector

Lauren Zabierek
Executive Director of the Cyber Project, Harvard Kennedy School's Belfer Center

CSIS EXPERTS
Emily Harding
Deputy Director and Senior Fellow, International Security Program, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

Emily Harding:

Hi. Thanks so much for spending part of your Friday afternoon with us. We have three great guests today to talk about revolution in intelligence affairs. This is part of an upcoming report that CSIS has on how a trio of technology can do amazing things to revolutionize intelligence. We're looking at the combination of open-source intelligence based on the cloud and enabled by AI and ML. And we decided to give it a friendly name, because this trio of technology can sound a little bit intimidating. But what we have in our mind was the model of J.A.R.V.I.S. Tony Stark needs help all the time, and J.A.R.V.I.S. is his wry companion who can answer any question in a moment's notice. And I was an analyst for a very long time. And I always said I could finally retire when J.A.R.V.I.S. was a reality for the intelligence community, when you could walk over to your desk and this beautiful display would pop up, and you could manipulate it with your hands and see all the data in front of you. So, when we imagined J.A.R.V.I.S. for the intelligence community we decided to call it OSCAR, Open-Source intelligence Cloud-based AI-enabled Reporting for the future of intelligence. So, in this report that we have coming out we provided about two dozen actionable recommendations on how to help analysts and operators understand what OSCAR can really do for them. And the idea was actionable recommendations, how to jolt the bureaucracy out of complacency and into the revolution that needs to happen. Our three guests today are old hands at sparking revolutions and innovations in their respective fields, both inside and outside of government. First off, we have Robert Cardillo. He was the director of NGA from 2014 to 2019. His other leadership positions include leadership with the chairman of the Joint Chiefs, DIA, and ODNI. He is famous within the IC as an innovator. Many of you watching today will know of the legend of Chris Krebs and what he did to really push CISA forward and be an innovator. Robert Cardillo did all of that inside the IC. And people speak of him with awe. You know, he was able to fight the bureaucracy and make amazing things happen. So, we're really thrilled to have him today. We also have Lauren Zabierek. She is the executive director of the Cyber Project at Harvard Kennedy School's Belfer Center, my alma mater. Very thrilled to have her here today. She was an Air Force intelligence officer and a civilian intelligence at NGA. And if you don't follow her on Twitter, you should. She's got this positive and inspirational Twitter feed, including featuring some of her excellent work with places like #ShareTheMicInCyber. We also have Sean Roche. He's the associate deputy – was the associate deputy director of CIA for digital innovation from 2015 to 2019. And that is a mouthful of a title – associate deputy director – so those who don't know the way that the IC bureaucracy works, that's a really big-deal job. It was his responsibility to lead everything from R&D to operations in the cyber domain. And he was also responsible for shaping that mission for CIA. He's now the director of national security at AWS in the International Public Sector. And thrilled to have him here today. So, I've asked each one of our guests to say a few words about this cluster of technologies in driving innovation. So, we'll go through a few words from the three of them and then move onto questions. And so, Robert, I will turn it over to you first.

Robert Cardillo:

Thank you, Emily. It really is a professional privilege to be here to have this conversation with such good colleagues as Lauren and Sean. And I know

we're talking about the future. Don't be afraid of my first sentence. The community that we all are a part of, and we are committed to its continued, you know, growth and sustainment and relevance was arguably born 75 years ago. 1947 actually legislated through executive order, at the time, and then followed up with congressional action to stand up the Central Intelligence Agency. And really birthed the community that we all have been proudly served within. And I'm old enough to say that I served about half that time. I guess I joined at the 37-year mark of so, in the early '80s, under President Reagan. But the reason I bring up that frame of reference is that I think it's important about how we think about going forward. Because we're going to talk about some challenges. And Sean and Lauren will know more on the technical side and will have also experienced what I'm sure going to talk about as some of the cultural inhibitors, what I call the unfortunate muscle memory that we sustain. But I think it's important to understand where that comes from so that as we seek paths forward that we take on that – I think the reality of that history, in order to make the changes that are necessary. So if you go back to that timeframe, it's no surprise that the community that we – that we represent was formed by the time in which it was created, which was a split world, literally and figuratively. Our key ally, Winston Churchill, described it, you know, as having an iron curtain in between the two worlds. And when you charge an entity, in this case the Central Intelligence Agency, with helping to understand what's going on on the other side of that iron curtain, you are shaped by the necessity of collection, right? You have to go and steal access, insight, understanding of the adversary. And by the way, yes, I'm completely biased given my history, but I think this country and our allies can and should be quite proud of what the CIA and the – and our pioneers did in order to create the insight in which there was none. And so, this is everything from, you know, early access to the atmosphere, you know, through the U-2 program. And then the CORONA program and putting intelligence capabilities into space when no one knew how to do any of that. And look, this old photographic interpreter can remember being excited because film was being dropped through the atmosphere in a capsule, being – deploying a parachute somewhere over the Pacific Ocean and being caught by an Air Force transport plane with a trapeze on the back of it. Now, that sounds nuts. And I think it's amazing. I mean, it's – I mean, it's American ingenuity to say, how are we going to see the other side? And I just say all that to say that a lot of the things I think we're dealing with today, even though – look, I have the utmost respect for my peers and those who have succeeded me in leadership positions. I think intellectually I think our intelligence community understands everything that we're talking about today. I think they appreciate the import of this conversation. And I think they are leaning in. But the reason I bring up that history is that I think we need to confront that core DNA with respect to collection. Now, by the way, I know we're going to be getting into a discussion, and hopefully a little bit of a debate too. I am not arguing that we need to get out of the collection business, OK? I'm arguing that actually we need to get way better at the collection business than we ever have been before. But when I think about open source, unprotected data, I think of less about collection more about access, verification, and application. So, the question really isn't, you know, how do I get that information, but really how

do I think about it? How do I contextualize it? And how do I present it in a way that's meaningful to a decisionmaker. And I'm going to finish there because, quite frankly, that has not changed since 1947. To my mind, the reason we have an intelligence community is to provide information at point of decision to improve outcomes – period, end. Yes, it's different today. Yes, the world is full of information and misinformation and disinformation, and all of those things that Sean and Lauren spend a lot of time on. But the core value proposition of our community hasn't changed. And so, to me, I think it's such an exciting time to be able to be thinking how we could elevate our mission – not eliminate it, not replace it – but elevate our mission in understanding adversarial capabilities and intent. Again, which is our core reason for being. So let me stop there, Emily, and look forward to this conversation with our friends and colleagues.

Ms. Harding: That's great. Any conversation about the future should be very much grounded in the past, and the wonderful, storied history of this community. So that's great. Lauren, over to you.

Lauren Zabierek: Awesome. Emily, thank you so much for, you know, having me here today and for your very kind words. You know, I'm not sure, but I have a feeling that Emily invited me on here because of how just fervent I was in my comments in a previous workshop. So, again, thank you for that. So, you know, if – as Emily mentioned, I was an Air Force intelligence officer and I was also an analyst at NGA. I did – I was in the office of counterterrorism, where that office revolutionized tradecraft and had developed the methodology known as activity-based intelligence. And so, we can go into that, you know, in future discussion, but, you know, I just wanted to couch that and just put it out there. But, you know, I just want to say, if my time in government, you know, really taught me anything, it's that people are our greatest resource. In the intelligence community, they are the ones developing tradecraft, making those hard decisions, doing the analysis, making the relationships that are necessary to break down those silos and to really innovate those new methodologies. But, you know, far too often, you know, from what I saw, you know, in my decade-plus, is that I think we failed to put humans at the center of those policies. You know, we haven't given analysts and officers, I think, the tools that they need to operate on the unclassified domain, the incentives to innovate. And, you know, pushing forth the policies that reflect the realities, you know, now of what data looks like and really the technology landscape, while also still protecting the officers themselves, you know, as well as the public. And so, you know, having read the draft, you know, and been a part of these discussions, I really think this paper is spot on. You know, for – as it, you know, discusses, for so long, you know, OSINT was really thought about, you know, as the news, right? We didn't want to be news reporters. But I think the revolution and now these sensors have been sort of democratized and commercially used and proliferated has been really too fast for the community to keep up with. And especially it's not just, you know, the people in, you know, the systems, right? It's the laws, and the policies, and the tech infrastructure that people are dealing with. You know, and I think also for too long, you know,

there's just been this fear of getting on the internet safely, right? The lack of tools to do so, and the lack of training, you know, how the internet even works and what the threats are. More than just, you know, you're yearly, you know, computer-based training, right? And so, I think that fear of doing something wrong, you know, really has created this risk aversion, you know, coupled again with the wrong incentives which, you know, I'll talk about in a second. But I think the concept of OSCAR is great. And, you know, I was thinking about this. And it's something that when I left the IC, which is a story in itself – (laughs) – I joined a cybersecurity startup. And, you know, we were trying to bring something very similar to the community. And that was this, you know, essentially data within a cloud-based system that, you know, we tried to say, like, look, it's protected. It's within the system. You know, you're not going to be exposed necessarily, you know, to the – to the wild, unclassified internet. But, you know, there were challenges getting people on there. Who owned the program, who decides what analysts can get on? You know, was it a program manager just sort of managing that, or, you know, it might have been better if it was sort of distributed, everyone could do it. You know, I think for too long it's just been sort of held in leadership and not, like, given to analysts to just play with, like? Like, look at trade shows. It's never the analysts that are there. It's leadership. You know, thinking about things like licenses, and, you know, how are those logins themselves apportioned and governed. Training too, both, you know, as a tradecraft for open-source intelligence. And here, I wanted to say that I think it's really important to understand that OSINT is inherently multi-INT, right? It's not just like, OSINT, there you go. You have to be able to know all how to collect and analyze all of those INTs therein. But also, you know, hands-on training for this particular cloud-based environment. And again, you know, the internet itself, who decides what is collected and brought into this environment? How is it collected, et cetera? What would the rules be for governing that data and, you know, for parsing out U.S. persons information too, if that's inadvertently collected. You know, what will the protections be if someone, you know, accidentally is exposed to that? You know, I think too it's important to understand, you know, the legislative environment or the legal environment when it comes to data right now. As we know, there's no national privacy law. You know, and companies can buy and sell data to really anyone. So, I think there's a lot of things to still work out on that side too, and how that would reflect within the intelligence community. And then finally, you know, I wanted to note about how analysts are actually incentivized. You know, I think, you know, at least in my experience, what I used to see, and I always talk about this, because in my office – in my counterterrorism office, they removed the burdens of production, right? They said: You don't have to worry about writing X number of reports. And while that may have hurt us for, like, promotions later down the road, they still very much focused on, like, did you come up with, like, a new way of doing something? Or did you come up with, like, a really important analytical outcome? Like, that was the focus there. And my old boss used to say, you know, what are – let's think about the off-ramps to production, but that's not the ends, basically. And so, I think the incentives there, you know, those are qualitative. They're not quantitative. And I think it's a lot harder to rate on that, but I think in that case, you know, we just need more people. And

people, are always, you know, in need in the IC. So, you know, we can get into that more too, but, you know, those are some of the things that I'm thinking about with OSINT. You know, again, it's been a couple years since I've been in the community, but, you know, I truly appreciate the ability to be here today with Sean and Robert. So, thank you, Emily.

Ms. Harding: Fervent is a very good word. I would have used compelling and eloquent, I think, for your earlier comments. And your point about people is very well-taken. We're going to hopefully circle back to that later and talk about both recruiting these excellent folks and then also once they're in the door giving them the space, as you're talking about, to play with the new technology. Because if you have a PDB due in two hours that is not the time to try to figure out a whole new database, right? OK, with that, Sean, over to you.

Sean P. Roche: Well, I'm honored to join this panel today. And I'm also really challenged now, because the first two speakers, Rob and Lauren, have really nailed I think every point I was going to make. So let me try and figure out how to add and maybe to double down on some of those points. First, what I really like about this is that it's – this study – is that it's action-based. You know, a long time ago Sheila Widnall, who was secretary of the Air Force, said: Two thirds of the Earth's surface is covered by water, and one-third is covered by studies of how to fix the launch problem. And it was such a big problem. And everybody knew it was. We only had one company. We had launch failures. Look at where we are today, with SpaceX and with other companies. Look at how it's changed. The price points, the access, the – SpaceX just had a launch the other night, another successful launch. Done very differently. So, the first message I have on OSINT and on this study is I'm a professional optimist. I just really think that it's time to move out and we can make progress very, very quickly in a way that changes sometimes what look like very, very rigid models. The other thing is, I really am glad that the first two of my colleagues mentioned people, because my message is to any analyst, especially our analysts in the field way far at the edge – which is where I enjoyed spending time – is: You deserve better. You waited a year and a half to get a clearance. You turned down a lot of other offers. And I got you using Lotus Notes? You just deserve a lot better. And I can't have you going home at night with a better internet connection and better access to peer-reviewed journals, et cetera, than you have at your desk in the digital workflow. And so, when I think about this, I see no lack of innovation across the IC. It's wonderful. You can find innovation everywhere. I think the key for OSINT especially is where that innovation is happening, what is the path to get that to scale? And the tools exist. You know, infrastructure is a service and the tools we have exist. But I've seen people doing remarkable things with OSINT in backroom somewhere. And they say: Don't tell the boss, because I don't want to have to fight my way into the baseline, and I'll get crushed, and it's too hard. Other times, it's one or two advocates are doing something really different, and their messaging might be a little clunky. And the rest of the folks hear: Hey, OSINT can replace you, or OSINT can replace our exquisite collection. And as Robert said, no, it just allows us to use that exquisite collection much, much better. You know, if you're a SIGINT person, your life is about moving from a Pri 3 to a Pri 2 in priority on the tasking. Otherwise,

you have to get someone to allocate a receiver to what you need collected. It's with things like OSINT that actually you can make that case and hone that targeting to the point where you get an exquisite product. And the PDB was mentioned. Talk about deserving better. On a 24-hour cycle, that in some cases ended up with the color printer being the pacing item for success. So, I really think that across the board, you know, the message has to be: You deserve a lot better. And I don't think there's anyone leading the community today in any agency that wouldn't support that. And I like that the word fear was mentioned. You know, I used to teach my folks that, you know, your job in getting change through is to get people through the cycle. And the cycle is fear, anger, denial, bargaining, acceptance. And we have meetings that said: Where are we? And sometimes we were still down in fear and anger. AI strikes fear in the heart of some folks, but then it strikes anger when you do the messaging incorrectly. I remember a senior making an investment in an AI/ML platform, a large investment, and said: We don't have enough analysis, so this will help us bridge the analyst gap. And what the analysts heard was: You're being replaced by a machine, which is absolutely the wrong messaging. Wasn't intentional, but obviously that initiative – that was \$120 million with zero return. So finally, the magic is not in the technology. The folks who sell the technology programs – and by that, I mean get funding for them – are in a mode sometimes where they make the technology sound magic and the technology sound special. It is not. It is the tradecraft that the analyst and the case officer, the people who actually execute that mission both operationally and in analytics, that is the magic. That is magic. So, our discussion and the actions – what I really like about the study is it hits to what do we do to get better tools to enable tradecraft.

Ms. Harding:

Thanks. That's really great. Yeah, we were seeking actionable. And this idea that technology is oversold at times – in some of the interviews that we did we spoke to folks who were very senior. And they said, you know, we've been sold a bill of goods so many times about what this can actually do. And then we see it in reality it's disappointing, and so it kind of gets shunted off to the side. And what we really need is an adequate understanding of what's possible and to get excited about what's possible, because it is really exciting. Just to get there, to get our mental faith there. I wanted to start off our questions with a very fundamental one, which is: What is open-source intelligence? As we did the lit review, it's very often defined as what it's not as opposed to what it is. It is not the classified take. It is the other stuff. Well, what's the other stuff? And as Lauren mentioned, you know, as I was coming up in the ranks, it was CNN-INT. It was the stuff that pops up in breaking news from wherever it was around the world. And we were always told: Don't try to be CNN, because guaranteed you're going to be at least 12 hours behind whatever has appeared on the news. And if you don't have anything to add value to the CNN reporting, then you shouldn't be writing. And it was always our goal to say, OK, this is the breaking news, but then how do you take your expertise or whatever classified reporting you had, and then add the context that was necessary so that the policymaker could not just make a decision – a snap decision based on what was on cable news, but something that was a little bit more informed by the longer view. But now open source

is something very different. It's not just press reporting. It's not just foreign press reporting. It's not just CNN-INT. So, I want to start with Robert and talk about what you see as open-source intelligence. The report that was before this one, the intelligence ed report was excellent, and laid this wonderful ground view of everything going on in the intelligence discipline. And it advocated very strongly for elevating OSINT. Say a little bit about that.

Mr. Cardillo:

Thanks, Emily. It was a privilege to be part of that study. I also should be quite clear that that august group could not agree on that definition. I'm going to give you mine here shortly, but you should read the report to hear from John McLaughlin and Joe Votel, and Stephanie O'Sullivan. See, I don't even like the term, frankly, because I think it – quite frankly, I think the term sometimes gets us stuck. And I prefer unprotected data. And the reason I do is because it just divides the world into one of two categories. There's stuff out there that's being protected by an adversary, or a system, or a machine, and, shoot, the Earth, you know, in some cases. And there's unprotected data, right? It's the things that are kind of generally accessible. Now, we can talk a lot about what – why Robert said “generally,” and, you know, where' the line. But for now, I'm going to use that term. And the other thing is, I guess, Emily – and you said this as you described your history and I don't disagree with it, it was my history as well – we used to sprinkle open source or unprotected data at the end, right? We'd finish, you know, our highly classified report, and then we'd take a look around, read a paper, watch TV, you know, and add something. And I think that has to be fundamentally flipped. I think – I think we need to start with accessible data. I think it needs – and, by the way, we had a debate within our study too about, you know, should it be in – should it be a place, right? You know, should we have an entity called open-source stuff, or agency, or department? I was in the camp of no. That it's everyone's job, and that it needs to be embedded in everyone doing their job. Now, I didn't just say we don't need discipline specialists and imagery and signals. Of course, we do. And of course, you would – you would have specialists that could do, you know, unprotected data searches in a particular way. But I think it should be every intelligence officer's job to access, and to leverage, and then to build on top of that accessible data with the exquisite that Sean mentioned. And not to, again, try to out-CNN CNN, but go back to our core reason for being. Information that discriminates a decision, you know, to create an outcome. And that's – again, it sounds – I don't know if it sounds simple or not, but to me it's very clean. And I'm just a big believer that – you know, and I'm glad that both Lauren and Sean brought it up – that if we just find a way to make it accessible and not such – don't make it so hard, I think the analysts will gravitate to it. I will say this, though, because, you know, Lauren, I heard you with your – you know, the rating issue about, you know, counting production. And, of course, I lived it myself, and then I wrote the policies that you were probably railing against at NGA. I apologize for that. But here's the challenge, right? You know, I think – I think one of our – I think one of our problems are is that the entirety of our evaluation system is negative based. Meaning, my experience was the best way to get to GS-13 was not to make any GS-12 mistakes. It was not to be a GS-12 hero. Now, did we have GS-12 heroes? Of course, we did, right. But more often than not, people were being careful because they knew, boy,

one bad step here and I'm not – I'm not getting promoted. And so that's probably worth talking about, because I do think that that does inhibit people from diving in, because it just looks risky. But I'll stop there.

Ms. Harding:

I definitely want to come back to the risk piece at every level, because there's the junior person risk, and then there's the senior person risk, and then there's the – I came from the Hill after my time in the intelligence community, and there's definitely the Congress is going to hate it risk, which I suspect is overblown. But we can get back to that. Sean and then Lauren, can you talk a little bit about what this wide world of OSINT looks like? Or unprotected data looks like? It was mind blowing to me when I first started to explore this area the variety of information that was just out there and useable. So, Sean, any thoughts on that?

Mr. Roche:

Well, it's really incredible. People talk about the growth, but – and the growth is certainly there, different types of data being available. What's really fascinating is if you look at the internet and how the internet works, Lauren mentioned that we don't spend enough time helping our people understand that. Since 1993, what really is fueling the tremendous growth in revenue – in billions of dollars of revenue – is the data that is inadvertently created via what is now all in a digital sense, an increasingly digital sense, of everything we do in our lives, which is going digital. And what I mean by that is, there's an incredible hyper-accurate stream of metadata and sub-metadata that are out there that can be – usually can be purchased, and a lot of companies who curate that data. They will do minimization on it to protect against collection from citizens, et cetera. But this is a huge industry. You know, when I go back to Silicon Valley now, in the San Jose area, where I spend a lot of time, where one of my jobs was to build exotic and amazing NRO satellites. Those factories have been bulldozed and there's a giant Google center there. That's the exquisite and increasingly exquisite generation of data that we couldn't imagine we could get. And so, I really – not only is the volumes there, certainly. But one of the issues for a lot of folks is, beyond handling the volume, is really asking the question of: Would I be able to discern this at the following information based on the stream of data that's out there? Now, to the point of collection and definition, I had the very unfortunate tasking at one of my jobs, is I had two people not come back from an operational environment. And you have to talk to a lot of people when that happens, obviously. So, we had people – we asked people to conduct acts under covert and clandestine authority that are a risk to them, that are a risk to the United States. And my mantra is: I would like to make those decisions very carefully and only when absolutely necessary. And whether it's a satellite that is dysfunctional and needs to be blasted out of the sky because it's going to release poison gas – you know, the fuel left in it – or whether it is some amazing member of the IC who is asked to go forward into a tough environment, we really need and owe people and our oversight committee that those decisions were made the right way. So, if I can boil down risk by getting data to help them be more accurate, help them being on the X for a shorter amount of time, to help that targeting, that's what – to me, what OSINT is all about, and has to be about.

Ms. Harding: Absolutely, to preserve those resources for the times when you really, really need them. Yeah. Lauren.

Ms. Zabierek: You know, and Sean, I just – I wanted to say that I really appreciate your comments on, you know, the analysts themselves, and making sure the people have what they need. And, Robert, I – (laughs) – appreciate your comments on the leadership aspect of it. And I do want to say that I know that it's more sort of mandated by Congress too, right? It sort of blows all the way down there. But I will say that, you know, I also agree with your point that it is everyone's job. So as an activity-based intelligence analyst, that's what we – what's what we thought, right? Everyone should know how to do every single INT, how to collect it, how to analyze it, et cetera. And certainly, there should be room for specialization, of course, but just wanted to make that point. So, you know, I read through, you know, all the different definitions of OSINT itself. And, you know, I will say that I think it's this tradecraft, and I think it's a set of tools, and the technology and the policies to really consume and analyze. You know, you mentioned the volume of data, Emily, but, like, the variety and the velocity of that data too. It's exponentially increasing because, you know, I think one thing we have to sort of keep in mind here is that the internet itself is a sensor, right? It is, like, the best – or one of the greatest sensors ever sort of invented. But there's a lot of issues with the collection and all that. But you know, I want to go back to my point about it being multi-INT too, right? Because it's not just news, right? You have commercial satellites, you know, doing imagery analysis. And there's, you know, commercial signals and commercial, you know, snippets of audio, right, and snippets of video, and things like that. And, you know, judging the veracity of human-derived information, you know, the writing, right? So that's HUMINT, right? So, you have to be able to do all of it to, I think, adequately, you know, understand and use OSINT in your – in your analysis. But, you know, and I also agree with this fact that, you know, sort of starting from that point. As ABI analysts, we wanted all of the data that we could get our hands on, right? That's where we started from. And we had a whole methodology to actually deal with what that meant, when you had all the data. But yeah. And I just think, you know, you're now swimming in it, as you said. And so – you know, as there was a point made earlier, there's technology to help parse through that, and help to deal with that. And I think that, you know, as someone who had tried to sort of bring that into the agency at one point, like, we had to do a better job at sort of embracing that and being able to use it in that way. But I also – you know, to my point earlier, you know, getting it to the analysts, right? Like, letting them – letting them use it. And I think – you know, I wrote a piece last year basically talking about the creation of, like, an intelligence community innovation unit. And a part of that was to be able to highlight great work being done across the community, and then helping to scale it out, I think, to Robert's point. I think because there's so much stuff going on, and good stuff going on, that we need to be able to see that. And I think too where there – I think so many analysts want to be doing really cool things with technology. And it's, like, if you say, like, look this is what we're doing and, you know, actually scale it out and show people, then I think that would help to go a long way.

Ms. Harding: Yeah. So, Lauren, it occurs to me that some in our audience may not know what ABI is. Could you say two words on what that is and why it's so great?

Ms. Zabierek: Yeah. (Laughs.) So, I'm definitely a nerd about it. So, ABI is a methodology called activity-based intelligence. So, at its core, right, it just recognizes that we are no longer in that Cold War mindset, right, that you have to analyze every single piece of information that comes in, right? That used to be true, because you had limited assets and limited analyst capability. That's, you know, not the case anymore. And so, there's four pillars to it, georeferenced to discover, sequence neutrality, data neutrality, and integrate to exploit. But it just helps you sort of deal with this, you know, ubiquitous data, and help to identify, say, targets or patterns of life, and things like that. But, you know, has certain – certainly has applicability to a number of different issues sets across the community.

Ms. Harding: Yeah. A decade, or more at this point, ago, Carmen Medina used to always say that the future belongs to the hunter. And the idea was not that you could just sit at your computer and let the data come to you, and you could read everything that comes in, because that's impossible. You had to go out hunting for the information that you think you need. And in this case, what we're talking about is having OSCAR, our J.A.R.V.I.S., help you identify what that information is. So, you had a tipping and queuing function where this assistant can say, no, no, no, look over here. Like, this looks bad, maybe look at this first. One of the things that I found mind blowing in the realms of data that were out there, The Washington Post did that piece on tracking Donald Trump's movements when he was president by tracking some of the cellphone data of those presumed to be in his entourage. And they could match up what they decided was probably a Secret Service agents cellphone with movements of the president all around. And if somebody can find the president of the United States that way, I mean, the possibilities are endless. Now, the Post's point was data privacy is something we should be really focusing on here, people. But it also has exceptional uses for the intelligence community, who have spent lots of money and time trying to figure out how to do similar things with assets I want to shift for a second and talk about that culture point that was raised earlier, because while the tech is outstanding what we're really talking about is adapting the culture so that it can absorb that tech and absorb it quickly. So why do we think – what do we think are these cultural obstacles to the absorption of these technologies? And I want to give a quick shout-out for anybody's who's interested. Corin Stone, who was a great intelligence officer, is taking a year to think the big thoughts and has written a wonderful series of papers that are out there. She wrote them through AU. So, check those out if you want to learn more about this. But for our panelists today, I'll start with Sean and then go around the horn, what do we think about when we think about the cultural obstacles to incorporating these changes?

Mr. Roche: Well, I don't think anybody in the intelligence community comes in with the idea that you come to the work in the morning thinking of how they can block something or stop something. And I don't think there's a collective

mood that we – you know, collective, organized effort to stop OSINT. However, I do think what is – when we talk about culture, the point I would hit on is there's a couple mechanisms that – and a couple gaps in those mechanisms – that need to be addressed. The first one is, and somebody mentioned it, we got huge volume. We got huge variety. But also, the veracity of the data. So, the pedigree. The thing about the exotic collection systems that the IC builds and operates is they know the pedigree of – from tasking to collection. They know what happened. One thing on the OSINT is you get a lot of pitches where it's flash magic without a discussion of here's now we vetted the data and here's how we know the pedigree behind it. And that's really important. That's vital in the intelligence process, and being able to understand your source, and being able to speak to the accuracy of the source. So, the people selling those datasets, they're motivated to sell datasets. So there has to be a harassing function, number one. Number two is, there's got to be a lot more robust ability to move it between networks, primarily the discussion is between the low-side and the high-side. Cross-domain solutions that also have a sanitization and quarantine. These are – these are – there's companies out solving this. It is a big area right now of investment. There's a lot of VC investment. But if you can't move it around the networks easily, and you have a giant, you know, infrastructure to service network and you can't move it, well, that's a blocker that – it's easy to use that as a reason that it's just too hard. And the third thing I'd say is the procurement model. And the procurement model today says: I build an application. And at CIA a lot of them are built in-house because it's on, quote, high side, so I got to build it in-house. And I build an application. And these folks, you know, trying to do this stuff. I used to say – when they worked for me, I'd say, you know, I have a team building – I have a team of thousands, literally, building applications that tens of thousands of people tell me they don't like. So, build the app, then go out and collect – gather the data. And the piece missing there is curation. And finally, you know, build an IT staff. And when you go to procurement and say, here's a turnkey way to do this today, that does not fit their model and it kind of blows their mind. And somebody mentioned licenses. When you go to subscription services, this also is a perplexing – this doesn't look like what we normally do. And, by the way, you're now combining things. When the company curates the data for you it does the minimization, it does the pedigree. Well, then that doesn't fit our organizational model. So, I think the cultural impediments come from some really – some integration mechanisms that don't exist at scale to get you to scale.

Ms. Harding:

Yeah. One of my favorite lines from the workshop was – from a former IC officer – was: No one does perfect like we do perfect. And the idea was that if you're building a bespoke tool on the high side, then that was something that you could create that was exactly what you thought you wanted. But you're right, quite frequently it turns out that that's not what anybody actually needed. All right. Robert let's go to you. What aspects of culture do you see as problematic here?

Mr. Cardillo:

I would say there's still tyranny of classification. It might be too strong, but what the heck. And what I mean by that is generally speaking a confidential

report is viewed as more valuable than an unclassified report, and a secret report, you know, better. Top secret and, oh my goodness, it's compartmented, oh, it's awesome, right? Because it's compartmented. And, by the way, we got some other special things. So, now, look, you know, I'm making light of it a little bit. And, let's face it, my colleagues will know there's a reason why those words are associated with those reports. And but I guess it goes back to the mindset. Because we – and Sean talked about acquisition. Sometimes we know how much we spent on that compartmented report, right? (Laughs.) I mean, and it usually began with a B, right? And so, let's – you know, there's – I guess – I don't know if this is cultural or maybe it's just financial attentiveness. I don't know what it is, but we say: Well, we better make sure and, oh, by the way, that the Hill sees how much value we're getting from that when we want to get funded next year. And I don't know. Again, I might be wandering away from cultural, but I do think these are inhibitors. I think they're realities that do inhibit us grasping it, because – this might feel like a non-sequitur – but, you know, look, when COVID hit hard in wave one, 85 percent of the NGA workforce was sent home to protect them. And then they were told to go to work at home. And by the way, they just had a director, you know, me, championing open and succeeding in the open, and trying to, you know, be better at unprotected commercial imagery, et cetera. But to, you know, Lauren's point, we hadn't given them the tools to do that. (Laughs.) And then we didn't give them the training. And so, now, by the way, I'm not criticizing my successor or NGA leadership. I think that's the reality of today. And so, I know you asked about culture, but I think when we continue to not fund things like – in the DOD world they're common access card readers. You know, things that can just, you know, make life – to Lauren's point – to safely access the internet, right, and to at least be able to give you some sort of protection. Those weren't funded the way those billion-dollar collection systems were. And so, I do think it comes back to mindset. And I guess I'll finish with the cultural piece. We have to find a way – maybe Lauren's leadership in her – in her CT role – that was outcome focused. I do appreciate it. You know, most of my life was spent with inputs, you know? How many of these, how many of those, over what period of time, and then you divide by a 100 and go, oh look, I'm at 78 percent of something. Well, sure. But the world isn't working that way, if it ever did. And we have to find a way to turn to outcomes and to value them and to reward them. You know, I think – I think the bottom line – I think you get what you reward. And today we're not rewarding the kinds of behaviors that we're describing.

Ms. Harding:

People have a really hard time wrapping their heads around culture, but all culture really is is a combination of policies and incentives. That is what shapes the culture. And the incentives are for cranking out the production and the policy is to do things that are safe and proven. And that's the opposite of where we actually need to be. So, I want to go to Lauren to talk about culture a little bit. I have a question about what happens if we don't do this. And then we have some questions coming in from our audience, which I greatly appreciate. If you haven't found the link already on the website, it's there. You can submit your questions. And we'll get a couple of those in just a minute. But, Lauren, first, over to you on culture.

Ms. Zabierek:

Yeah. I appreciate everyone's comments on this too. And I think, you know, Robert, you said something about this fear of, you know, not getting funded. I think that is a huge motivator for a lot of people, right? If you're, like, not, again, producing a certain amount of reports or, you know, showing X, Y, and Z success then, like, oh my gosh, you're not going to get funded, and you aren't going to get the billets, and duh, duh, duh. Like, I feel like that has to change. And I don't have the answer to that, but, you know, if – maybe if, you know, a certain block of funding, you know, was unchanged, you know, for personnel, right? And then – I mean, I don't know how the budgeting works in there. But I just know that that is a motivating factor there. You know, you quoted in the paper, Emily, this thing that I said. But I was quoting a professor, actually, here at the Kennedy School. I had taken his class when I was a student here, Stephen Goldsmith. And he talks about this more in, like, a city government perspective, but I – when I took this class I was like, on my gosh, this was, like, totally, you know, the things that I was thinking about as I was leaving the intelligence community, somewhat unwillingly. But he talks about the need for people in the system to go from being rulebound to problem solving. And that, I think, is the crux of what we're trying to do, what analysts should be doing, right? We're not here to just count things and write reports. We're here to solve problems, or at least, you know, do these hard things, right? That's what we're paid for and that's, you know, the people that we want them to do. And so, again, you know, coming down to incentives. And so harkening back to, you know, our leadership. Again, it was, like, what relationships, you know, did you make? What data, you know, were you able to get? What – you know, we had a number of deployment spots that we, you know, went out and created, you know, because we had those relationships with other organizations. Again, the analytical outcomes, the operational outcomes, you know. So, you know, a system that incentivizes those things over, you know, these numbers, I think, and other, you know, I'll say, non-numerical sort of attributes, and the way that we contribute overall to, again, getting that problem solving thing. But to answer your question on, you know, what happens if we don't do this? You know, I think that we're going to miss out, right? We're going to miss out on the ability to, at the end of the day, protect our nation and protect our people. And that's, like, you know, the top of what everyone's thinking, right? But, you know, from a very operational or even tactical level, we're going to miss out on information and indications of warnings. You know, I think one thing we have to take a step back and understand is, like, we're not in that old paradigm of conflict anymore. We are in – very much in this gray zone conflict. Like, it's happening right now. It's all around us. It's ambient. And so, if you don't have an eye towards what's going on outside of that classified bubble, you're not going to, I think, understand what's happening, and then be able to, you know, provide that information to the decisionmakers to then, you know, craft the right responses and policy.

Ms. Harding:

That was a great segue to our first audience question, so I will – I will do that in one second. But I also want to point out that this idea of being a problem solver, that is where the IC really excels. One of my friends who was a paramilitary officer used to say that the difference between the United States military and the paramilitary officer at the agency is that the U.S.

military will come up with an operation and train for six months to get it absolutely perfect. The paramilitary officers it's, like, eh, there's a problem over there. Can you guys just go figure it out? And that's it. Like, that's your guidance. (Laughs.) So, the improvisation and the problem solving, like, this is actually where the IC excels.

Ms. Zabierek: Well, you know, and if I could just expand on that real quick – and I know we have to get to questions – but, you know, when I was leaving the community, I mentioned it was unwillingly because I, you know, was trying to get a joint duty assignment as my husband, you know, came up to Boston and it didn't work out. So, when I left, I was, like, oh, what am I going to do? And I applied to the academy school because I was, like, I want to fix the intelligence community, you know? And so, this is just cool, that we're even talking about it. But I just remember this feeling of, like, within a certain part of the community if you ask – like, if you had an issue they were like, meh, the regulation says this, so can't do anything. Whereas another part of the community, where you used to work, Emily, they were like, how can we help? (Laughs.) You know, so there is definitely a difference there. So, yeah, it's – and, by the way, the book that Stephen Goldsmith wrote is called "A New City OS," so, like operating system. And it's a – it's a really easy read. So just a plug.

Ms. Harding: Thank you. There's activity going on outside my office. I'm going to apologize for the noise in the background. But we do have a question just on this from one of our audience members. In regard to recent escalations between Russia and Ukraine, posts on social media accounts were the first to report on troop mobilizations, dating back to spring 2021. We all saw the tanks moving on trains. How do you believe the emergence of open-source information, especially social media, played into holding governments more accountable and responding to the crisis? Anybody want to volunteer to take that super easy question on?

Mr. Roche: Well, any movement creates a digital field to collect that. And so, we know that the – in the bin Laden raid, the very first public acknowledgement was someone on Twitter saying: Do you hear helicopters? It's kind of unusual for this time of night. So, you are escaping the ability to swim through the digital – you can't. So, again, I think, you know, as has been pointed out, things are a lot – moving at a much greater speed with much greater agility. And open source has to be built into the current digital workflow on the high side as well. And today, you know, the two separate workflows, that integration is not going to happen fast enough. You can't – when I would go back to brief the Senate, there were times when they'd say: Come down in two days and tell us what happened. And by the time I got down there, using open source, they had 90 percent of the story – 95 percent of the story. So, it's all about speed.

Mr. Cardillo: If I could add, given the Ukraine scenario, I think the question cuts both ways. Meaning – you said, how does it hold governments accountable? I think there is a way to talk to that, through the exposure, transparency, you

know, shining a light on, et cetera. But, OK, this former Soviet analyst would argue in this case it's helpful to Putin, meaning he wants it advertised, quite frankly, that he's on the border, because it's creating exactly the tension that he's looking to create. So now I'm not saying that – by the way, that doesn't make open source bad. That makes the reality that Sean just described real, OK? The world is more transparent. It's more connected. It's more – it's more informed, right? I think the – I think then it becomes even more important to talk about tradecraft. Meaning, in a world that's flatter, more accessible, and more connected, and in a world in which we don't have as big of a technical advantage in space access and sensing and all that, we have to be better at our tradecraft. You know, and, you know, I used to challenge my team at NGA. I said, hey, look, we did great in the closed world. And I'm proud of our history there. I was part of it. How do we win in the open world? It's a different fight, quite frankly, because, to your point about, you know, Ukraine, is he parking those tanks so that, you know, the commercial image does see them, you know? And what does that mean, with respect to intent? And so that gets to the human nature of our business, which is, at least I think for a few more years, it's going to be tough for AI to keep up with. But thus, I think it goes back to our central point here. If you don't have the right talent on the team, we don't have a chance. I agree that we've got the right talent. But we've got to give them a chance.

Ms. Harding:

So, I'm going to try to combine two audience questions into one, since we're running a little short on time. Somebody asked, one of the biggest issues is that the government does not have a good document that lays out all of the official translations for key Chinese terms and concepts. What should we do to solve that problem? And I want to link that to the broader question, which is that if the intelligence community manages to pursue this idea of open-source intelligence from anywhere, where you can collect all of this open data, unprotected data, and pull it together in a really disciplined and analytical way, then what does that mean for having a broader customer base for that information? What does it mean for opening up some of the intelligence community's talent to different parts of the American government or the American people? Lauren, do you want to start with that?

Ms. Zabierek:

Yeah. So, on the first question, I think that probably exists out there somewhere, right? Somebody has to have it. And so, I don't necessarily think you need create a bespoke government solution for that. And that's, you know, where these partnerships, right, between the public and private sectors can really help. And they do. On the – can you repeat the second question? About data and the difference audiences, right?

Ms. Harding:

Yeah. If the IC can do open-source intelligence really well, then it's not classified, by definition, right? You could share it much more broadly than we currently share out intelligence products.

Ms. Zabierek: Yeah. So, you know, I've been thinking about this recently. I think that, you know, and I feel like Sue Gordon's talked about this a lot too. But, you know, the need for the government – the IC, maybe it's not the community itself – but the government to, like, talk more with the American people about what's going on, and being a little bit more transparent, right? Because there's still very much, like, you know, this veil around the intelligence community – for good reason, of course. But, you know, I feel like if there was just more sort of, like, interaction and communication, there would be less, you know, breeding ground for conspiracy theories, I guess you can say, especially, you know, what happened in the last administration, you know, with this politicizing and really disparaging of the community, which was really awful to watch, you know, from the outside. So, you know, I think just being able to communicate more, you know, with the American people. And that's something that open-source intelligence can do. And, you know, also on the flipside of that real quick, is, you know, because I've been in cybersecurity for a couple years now, like, everything basically is happening out here on the unclassified internet. And so, you have so much unclassified threat intelligence, right? So, I think it's a good instructive sort of use case for that.

Ms. Harding: Yeah. Absolutely. Sean and Robert, I will turn to the two of you for any closing thoughts you have. Thank you so much for being here. Sean.

Mr. Cardillo: A little negative and then I'm going to finish positive. Meaning you asked earlier, what if we don't do this? And you never, I never gave the burning platform at NGA. Oh, we're going to go out of business in a couple of years, you know, if we don't do X, Y, or Z with commercial imagery. For two reasons: One, I didn't think it would be very effective and, two, I didn't believe it, right? I didn't think we were going out of business. I was worried about going out of relevance. Meaning, Sean made the point earlier about, you know, you run down to the – run down to the Hill – 48 hours after the event you go down to the Hill. And they know most of everything you've got. And you're going to go, how much did I spend on Sean last year? And you know, he's incremental. But you know what? OK, that could be seen as a negative. I see that as a positive, because it's game on team. And I'm talking about the talented professionals that have succeeded each of us. And I'm betting on them. You know, to Sean's point, you know, our tech is amazing. You know, we've got this venture capital, risk capital, you know, entrepreneurial mindset that's very – by the way, you know, floating capsules through clouds and catching them with trapezes, we still have that. And so, I'm terribly optimistic, if – OK, here it comes – if we can unleash this potential and equip them. And it's not much, to Laruen's point, where the wherewithal, tools. It's not – these are terribly expensive. And the incentive structure. And that could be the hardest part. But I'm very bullish on the future. I think if we can just get out of the mindset of trying to out-China China and try to out-America China, I think we'll win.

Ms. Harding: Yeah. Absolutely. When I was at the agency, I used to when I needed inspiration go out to the SR-71 Blackbird parked in the parking lot and pet it,

and get inspiration from it, because it was a group of people coming together to do something that was crazy. That airplane is crazy. And hugely innovative and amazingly impactful. And I'm sure that when somebody presented the plans the first-time people went, what? No. Absolutely you can't do that. But there it sits. And still when it was retired, the fastest airplane in the world. So, if that can happen, this can happen to. This is also where I make the pitch for all of the data scientists who are watching this out there to come work for the government, tell your friends. It's really a great place to learn, and grow, and serve your country. And I loved my time working for the government. These other professionals on the screen did too. Thank you so much to the three of you for being here, for spending an hour on your Friday afternoon to talk about such an important topic. And hopefully we'll get back together in a couple years, and we'll have all kinds of tremendous progress to report. Thank you so much.