TRANSCRIPT

Event
“A Conversation on Cybersecurity with NSA’s Rob Joyce”

DATE
Tuesday, April 11, 2023 at 11:30 a.m. ET

FEATURING
Rob Joyce
Director of Cybersecurity, National Security Agency

CSIS EXPERTS
James A. Lewis
Senior Vice President; Pritzker Chair; and Director, Strategic Technologies Program, CSIS
James A. Lewis: We’re all set? Great. Thanks to everyone who came to CSIS. Thanks to the audience online for coming to listen to Rob Joyce. We were lucky to get Rob, thank you for making the time to come here. He’s coming from a bigger venue, so this is a little more – little cozier.

But we’re going to talk about any number of things, but I’m going to start by asking about NSA’s sort of new posture, when it comes to cybersecurity, which I think is really interesting. And we will have time for audience questions. If you’re online, I think there’s a button that you can submit a question on. If you’re in the room and you want to raise a question, raise your hand, and we’ll give you a card. We do filter the questions, so.

Oh, and I have a – if you’re doing it in the card, please write legibly. I can’t read anymore, so. (Laughter.) It’s not clear I could ever read, but if I mangle your question, it’s your fault. (Laughter.)

But with that, Rob, how long have you been at NSA?

Rob Joyce: So, first, Jim, thanks for hosting us here. Appreciate it.

Thirty four years.

Dr. Lewis: Wow.

Mr. Joyce: So I came straight out of college and –

Dr. Lewis: A lifer.

Mr. Joyce: – have been a lifer, and that’s not unusual for NSA. You know, the mission is spectacular. The ability to just work with really smart people, and work on hard, meaningful problems keeps people there, so it’s great.

Dr. Lewis: Did you see an uptick in recruitment with the downturn in the tech sector? I know there was some hope of that.

Mr. Joyce: We’ve gotten some uptick. What I would say is, we got some people of an experience level we didn’t often see. So we’re seeing mid-career people looking to come to, one, the stability, but two, also the opportunity to come into the intel community.

Dr. Lewis: Mmm hmm. That’s great.

So one of the things I wanted to touch on was, the NSA really has a new approach to cybersecurity. And I was thinking about it this morning, that it used to be called – NSA stood for, you know, “no such agency.” Now you’re so public. What’s changed?
Mr. Joyce: Yeah, well, it’s a recognition that we have intelligence capabilities that are vital to the defense of cyberspace. Industry owns and operates most of the digital landscape, and if we can’t figure out how to take the things we understand from that foreign intelligence mission, reaching into adversary space, and pulling down threats, tools, tradecraft, and information about those operations, and get them to the people who could do something about it, we’re not very effective, right? So it’s no good if we know something, if we don’t do something about it.

Dr. Lewis: So an Asian diplomat this morning asked me, what did America mean when we say active defense? When we say active defense, what does it mean to you? I gave him an incoherent answer, so – (laughter) – I hope you can do better.

Mr. Joyce: So it – so it means a lot of things. But the way I would describe active defense – I’ll give you a soccer or football example. You know, if you give somebody unlimited balls, and they get to sit at the, you know, outside of the goal, and just kick, and kick, and kick, and the goalie’s got to stop kick after kick, eventually, they’re going to score. And the idea behind active defense is, you’re going to use tools and capabilities to make sure they don’t get to do that unimpeded. So you’re going to play defense.

Some of that is deterrence by denial. You’re going to work on your defense, so that we do the things we know we’re supposed to do, the basics – patching, two-factor – all of the things, you know, the new buzzword, hot buzzword of zero-trust – but there’s also an element of, you’ve got to go forward at the enemy, just like in the sports analogy. You know, some of that is taking it down the field.

And so for active defense, one of the things is that public posture of NSA, taking the tools and infrastructure from adversaries, and outing those with the help of industry, so that all of us work together to take away those capabilities. So those are pieces. There certainly is the element of Cyber Command may go in there, and take active operations that remove infrastructure capability. But they also go out and do hunt forwards, where they, at the invitation of other governments, come in, and look for malware, and then take those things out, helping to cleanse that network, but also then expose the tradecraft, the infrastructure, and the tools that they found in it.

Dr. Lewis: How much of the activity we see is usually done through a Western intermediary? So you’re in Russia, you use a Western cloud server; you’re using a European server farm. What – how much of that is going on?

Mr. Joyce: It is almost nonexistent that a hacker comes straight from one of the – you know, the big four nations – Iran, North Korea, Russia, China. Most
companies will have the filters and the firewalls to understand that that event is at worst suspicious – or at best suspicious, at worst, you know, malicious and you just need to stop it immediately.

But what we find is often adversaries are now renting servers, often through fake identities, to come in and emerge from a reasonable cloud-hosting VPS location or they’re hacking devices. They’re compromising things inside our wire, inside the fence line. So that, you know, they make a couple hops and then they pop out with a U.S. IP address and they come to do the attack with what is reputationally better indicators.

Dr. Lewis: So how much of this concerns supply chain trustworthiness? Where does that fit into your equation?

Mr. Joyce: I think we’ve got a number of examples. You know, you can think of SolarWinds and examples like that where compromise of a trusted device will get you access to a number of things. We saw what industry reported as the North Koreans in the 3CX IP phone compromise where they trojanized and went ahead and put malware into an update that an unsuspecting business would download in theory to make themselves more secure and opened a back door.

So that’s got to be part of the threat model for organization and entities. That’s why you hear about the defense in depth concepts that people are pushing out now so that when you assume you’ve lost trust in a device or a user or something along those lines it doesn’t compromise the entire system.

Dr. Lewis: And I should note my second to the last question is about TikTok but I’ll lull them into a false sense of security before I ask it.

I thought the buzzword of the week was resilience and we don’t – I can’t keep up. DOD keeps adding a word in front of deterrence like integrated deterrence, vegetarian deterrence, whatever. I thought resilience had taken the place of –

Mr. Joyce: So resilience is, certainly, a word that you want to have. I don’t care if you’re an individual, a corporation, or a government, right, if you can’t be resilient to the threat. A good example is, you know, people talk about phishing links and that if you click on the link – you’ve got to train your users not to click on suspicious links.

I’m the cybersecurity director at NSA, right. You could craft an email to me that would get me absolutely to click on that link, right. You just have to do a little bit of research and maybe come at me several different tries. But eventually I’m going to click one of those links. So that means you’ve got to
Design your architecture to assume the humans are human and that bad things will happen to build that resilience into your model.

Dr. Lewis: One of the concerns that has been expressed about things like ChatGPT is they’re going to do a lot better at designing phishing messages.

Mr. Joyce: I absolutely believe that. So people have gone across the scale of, you know, how worried should they be about ChatGPT. I will tell you the technology is impressive, right? It is really sophisticated.

Is it going to in the next year automate all of the attacks on organizations? Can you give it a piece of software and tell it to find all the zero-day exploits for it? No. But what it will do is it’s going to optimize the workflow. It’s going to really improve the ability for malicious actors who use those tools to be better or faster, and in the case of the malicious foreign actors it will craft very believable, you know, native language English text that could be part of your phishing campaign or your interaction with a person or your ability to build a back story – all the things that will allow you to do those activities – or even malign influence, right. That’s going to be a problem.

So is it going to replace hackers and be this super AI hacking? Certainly not in the near term. But it will make the hackers that use AI much more effective and they will operate better than those who don’t.

Dr. Lewis: Mmm hmm. That’s great.

I told you I was going to ask you about the Cybersecurity Collaboration Center, which I think you had me out to when it was brand new. How’s it going? What’s the intent behind it?

Mr. Joyce: It’s going great. So the intent is to operationalize the things we know with the people who can do something about it. So we have a center that is mostly unclassified but still has an unclassified portion to it. And what it does is it lets us interact with industry. I mentioned earlier, you know, they run and operate the internet. They run and operate the tools and capabilities that we all rely on.

So if we can take and understand a threat and get it to that ecosystem at an unclassified level – and that’s the key, because if I give a company a secret at a classified level, most of the time, even if the person receiving it is able to receive it at that level, the people who action it aren’t, and we can’t have it in the ecosystem and execute on it.

But what we work hard at is getting those secrets sanitized to the point they can be actioned. And we don’t just throw it over the fence. That’s the lesson learned from a few years ago. We used to take things we knew and pass it
through intermediaries, whether it’s other government agencies or the industry partners.

What we do now is we put two analysts together so that what we know out in foreign space is married with the expertise they know going on in their network. And those two will iterate and be able to do things neither is going to do alone. So, you know, when I take Russian tradecraft, inject it into that discussion, they may protect a billion endpoints against that Russian tradecraft, right.

And so now critical infrastructure, government, even us as individuals, are all protected against that tradecraft. But the company also brings back to us other things associated with that that we never would have seen because it lives in their ecosystem. They bring it back, and that makes us more effective at going and researching the next threat.

Dr. Lewis: That’s kind of a different approach to intelligence. It’s not the old-style signals intelligence.

Mr. Joyce: Right. It’s very different. What we know is not nearly as secret as how we know it. And we never unbundled that in the past. And that’s really kind of the mindset change with the Cybersecurity Collaboration Center.

Dr. Lewis: So I was going to ask, what data has been most useful in these exchanges? What do the other people want to hear, and what are you telling them?

Mr. Joyce: So for us, when we talk classified to classified, the most useful thing is context. So there’s so much bad stuff out there in the ecosystem that these companies often don’t know what to focus on. And so if we can point to something and explain in a classified exchange why it’s a bad thing and why they need to care, then all of us can work in the unclassified space about the things we know about infrastructure and IPs and domains and tradecraft and malware examples and things like that.

So that’s one example. The second, beyond classified context, is just the start point for something that’s malicious. And, you know, if we can give the tip of where the analytics need to focus and then we both continue to unwind that ball of string, it gets to the outcomes that then illuminate the bad activities.

One thing we’ve found is we can work with one company one on one. They can bring their unique understanding, their intellectual property, or their perspective to the problem, and then they publish the blog that then illuminates all of the activity they know about. And then industry then dogpiles onto that and continues to tear that thread up. And that’s really a beautiful cycle to watch, where it starts from an intel threat to a company
that just grabs the adversary hard and then the whole community piles on and pulls it apart.

Dr. Lewis: So this is really an all-out unclassified activity.

Mr. Joyce: Mmm hmm.

Dr. Lewis: Yeah. And that’s really interesting.

So NSA had something called – I forget what it was – enduring security framework. I don’t know, nor do I care, if you still have it.

Mr. Joyce: We do.

Dr. Lewis: You do? How’s that going? It was all – it was like CIOs or CEOs. It was pretty senior.

Mr. Joyce: It’s CEOs. We get together in a public-private partnership. It’s NSA and CISA, and we pick an activity to focus on. So some of the work that’s been going on in the last year, there’s a series about 5G cloud security. What people often don’t recognize is when you want to do 5G security, you’re really talking about the concepts of securing the cloud, because that’s how the architecture is broken down. And we took telecommunications companies, high-tech, you know, vendors, brought them together with the government threat expertise, and put out a series of how you architect 5G for security. We’re now working on Open RAN as well, and a few other topics. So those are long-term, joint government and industry security efforts.

Dr. Lewis: What’s the difference between the collaboration center and ESF?

Mr. Joyce: ESF lives in the collaboration center.

Dr. Lewis: OK.

Mr. Joyce: So it is – it is a piece of that. The difference is it’s usually – when I think of the work of the collaboration center, they’re very focused on those threats. The threat actors and how do we – how do we give the threat actors a bad day.

Dr. Lewis: So the national strategy, the new national strategy, had a fair amount about securing the cloud in it. I mean, what would you – what would you suggest there? What needs to be done? It gets a mixed review when you talk to people who are customers, that some are secure, some could maybe be better.

Mr. Joyce: Yeah. I think the current push for secure by design is something we’ve got to apply to the cloud, right? And it starts with, I’d say, secure by default. For a
number of years, if you were going to spin up a cloud instance, it was often optimized for ease of use rather than optimized for security. And you had to be knowledgeable enough to lock down the components that make you actually more secure. Companies are getting better about the default being more secure, but we're not all the way there.

Dr. Lewis: How does O-RAN change your business? Because it’s going from – I was at a briefing a few days ago where they said that telecom is the last industry to really move from hardware to software, but they are doing it. So how does that change your business? Reluctantly, I might add, but – I'm kidding.

Mr. Joyce: Yeah, O-RAN is meant to – for those of you that don’t know, O-RAN is the Open Radio Access Network. So at the edge of your cellular networks, on those towers, is the radio portion that’s going to carry the signals from your cellphone to the tower. And often, you know, the big providers would deliver something that’s integrated from the antenna all the way to the whole switching fabric of the network. Open RAN is intended to kind of decouple the radio from all of the other stuff, with the intent to allow more competition in that backend, to allow essentially, you know, cloud computing folks to participate in the cellular networks.

And so the effort is to decouple those. You know, you saw us talk about the cloud security guidance. So between those two pieces, what we're trying to do is set the West up to be back and have options that are not Huawei, options that are affordable, supportable, and economically viable for the West to choose. There are good solutions out there, but when you go to a foreign country and they're looking at the bids, and there’s a subsidized bid from Huawei against, you know, the technology you can trust, you’ve got a really hard dilemma. What we're trying to do is offer technology they can trust at a level that competes more affordably.

Dr. Lewis: Sometimes when you talk to the big telcos they'll say that O-RAN isn't ready for primetime. Do you have a guess on when it might be? And they say scalability and reliability, because they can’t be, like, certain software companies and have blue screens of death, because their customers will flee. We’ve made it easy to move. What’s the timeline for you when you talk about O-RAN?

Mr. Joyce: Yeah. There’s O-RAN trials going on right now. And I think those are the key to getting that reliability. So the hope is the major companies investing in this and driving them to a security level they need, a reliability level they need, and a capacity will push that timeline.

Dr. Lewis: And all of them say they’re going to use it. No one has said O-RAN isn’t real. But it’s more a question of when does it get here? What would you do to improve collaboration with industry, both as a government and as an
Mr. Joyce: Yeah, so we're on that path. Our collaboration center is that experiment. We started with one company a little over two years ago. We're at 300 that we interact with, many of them on a daily basis in this analytic exchange. Hundred percent voluntary, right? They come because we deliver something that they find protects their customers, their networks, their brand, their reputation. Some are there for altruistic reasons, right? They want to help make the internet more secure. But in reality, most of them are motivated because it helps their business. So that's one thing we found, is we're getting this willing set of, you know, folks that can make a difference.

So what we've got to do is we've got to continue getting faster at being able to take the things that are sensitive and get them into the operational space. And today that's still a pretty manual process. And so that's where we're headed, is how do we take some amount of that sigint intelligence and have it automatically flow at the speed of cyber? Because that's really where we've got to be.

Dr. Lewis: Yeah. And not surprising, because I've heard that one before. One of the questions I was going to ask about the division of labor with CISA. At the start, back in the stone age of cybersecurity, when it was NPPD, tensions could exist between the two agencies. But it seems to be going pretty smoothly now, but how is the work relationship with CISA?

Mr. Joyce: Yeah. So, like anything, it's never perfect, but we are in a great space. You look at CISA, I don't envy Director Easterly and the CISA team with the size of their mandate, right? They have all of the federal civilian agencies but, more importantly, they have the critical infrastructure of the nation, and even the forward-facing, how do I think about making the ecosystem more secure? So that's a massive remit.

I have a smaller segment where we do that intelligence production against foreign threats, we work national security systems. So any system that carries classified information or is a warfighting system, those are things that we work on the security of. In the case of encryption, we develop and certify all the encryption for the nation. And then we have this defense industrial base focus, and that we leverage out into the ecosystem through the sharing. Those big companies that protect the Defense Department are the same ones that protect the banks, and the government, and others.

So I can be more narrow and more focused. CISA has the big piece. But our intelligence goes into CISA. We partner. You see one of the things we've done a lot of is advisories, where they'll be CISA, NSA, FBI, and, increasingly, third parties – second and third parties in there, where we talk about an ongoing threat and activity that we're trying to address. And so that unified voice
pushes us along in the protections we can offer. And that partnership is so much more aligned than it's ever been.

Dr. Lewis: I’m going to depart from the script for a minute by – because you brought up FBI. So this is your chance to give a 702 plus, a FISA plug.

Mr. Joyce: Sure.

Dr. Lewis: I think it’s going to be tougher this time. Everyone does.

Mr. Joyce: So FISA Section 702 is up for renewal this year. And it is a vital source of intelligence. It is an authority that lets us do collection against a known foreign entity who chooses to use U.S. infrastructure. And so it makes sure that we don’t afford the same protections to those foreign malicious actors who are on our infrastructure as we do the Americans who live here. And so I can’t do cybersecurity at the scope and scale we do it today without that authority. So we’ll be working hard, you know, with Congress, with the administration, with our partners at FBI and others, DOJ, to figure out how we get 702 reauthorized. It’s really vital.

Dr. Lewis: Well, I was going to ask you what you thought of the new national strategy, but of course you have to say it’s great.

Mr. Joyce: It is.

Dr. Lewis: Do you have a favorite pillar?

Mr. Joyce: I am fond of the pillar that talks about getting – taking it to the adversary, right? So part of the NSA – you talked about NSA change. One change is we created an organization called Adversary Defeat.

Dr. Lewis: Are you reading my notes?

Mr. Joyce: I am not. (Laughter.) So Adversary Defeat was intended to have a set of people who get up in the morning and go to bed at night thinking about how do I give the adversary a bad day using what NSA has or knows.

We in actuality don’t have a lot of authority to do stuff. We have authority to know stuff, and so we’ve got to have partners like industry, but also partners like FBI, Cyber Command, CISA, increasingly others like State Department, Treasury, and the likes, because we can bring pressure to the cyber actors through many means. And so our Adversary Defeat function is figuring out how we operationalize the SIGINT we know. How do we find the partner who could do something effectively, that takes an actor out of the ecosystem, or disrupts them from being able to have those free kicks on goal?
Dr. Lewis: What would you say are the big lessons? The word that triggered this for me was proxies. You didn't say proxies, but I thought proxies.

Mr. Joyce: I didn’t. (Laughs.)

Dr. Lewis: We could ask about that. When you think of adversaries, how many of them are state? How many of them are proxies? How many of them are purely private criminals? I mean, this – it’s hard to tell with the Russians, and some of the others –

Mr. Joyce: Yeah.

Dr. Lewis: – but with the North Koreans, it’s easy. But what’s sort of the blend here?

Mr. Joyce: I can’t give you a number. There is this scale that goes from black to white, and there are shades of gray all the way between.

I can absolutely tell you that, you know, there are nation-state hackers by day, who use their tools, and capabilities, and knowledge to do bad criminal things by night. There are patriotic hackers who have joined into the Ukraine-Russia fight, who are purely non-aligned. But there’s also a bunch of intel activity, where Russian hackers who work for the government, you know, do their – do their activity, and shroud it in the cloak of patriotic hackers, right? And so that mix gets exceptionally complex.

Sometimes, the foreign intelligence helps us sort those into piles. Sometimes, it doesn’t matter, right? Bad things are bad things, and whether it is nation-state or criminal, patriotic individuals, you know, you got to make it stop. And that comes in all elements of government power, whether it’s, you know, the law enforcement, if you can get and reach them, rewards for justice to drag them out of that space, whether it’s State Department doing diplomatic norms and engagements with their country, all the way down to Treasury, and the using the power of sanctions and OFACs. So it’s a wide array of tools.

Dr. Lewis: Did we overestimate the Russians? I think I probably did. When you – looking back at Ukraine, and the start.

Mr. Joyce: I think where the overestimation happened was the concept of combined arms. So the Russians in the physical space and in the cyber arena haven’t demonstrated the ability to do sophisticated use of complex things. And in cyber, you know, I think people have underestimated really how much game they brought, whether it be the Viasat hack, to, you know, nine or 10 different families of brand new, unique wiper viruses that have been thrown in the ecosystem.
So the things that are hot and ongoing today are, there’s continued – there’s continued attacks on Ukrainian interests, whether it’s financial, government, personal individual business, just trying to be disruptive. There’s a lot of intel collection. You would expect that, right, in an ongoing kinetic war, that they’re going to collect intelligence. There’s creative things going on. Like, we’re watching the Russian hackers log into public facing webcams to watch convoys and trains delivering aid. But they’re also hacking those webcams, where there’s zero days or end days where they can log in and, instead of using the town square that’s available to the internet, they’re looking out the coffee shop security camera and seeing the road they need to see. So things like that are ongoing.

And then when you look to the U.S., most of the pressure is at the defense industrial base, and the logistical transport companies who are moving lethal aid. So they are under daily pressure from the Russians. Again, that looks a lot like intelligence, right, to understand what the West is delivering, what the U.S. is supporting, what we’re doing.

Dr. Lewis: But so far they haven’t tried much in the way of disruption.

Mr. Joyce: No.

Dr. Lewis: OK.

Mr. Joyce: No, not over here, right, but very much so –

Dr. Lewis: Sure.

Mr. Joyce: – in the theater and the adjacents.

Dr. Lewis: Yeah. There’s some interesting lessons there about sovereignty and international law.

Can we duplicate the Ukrainian approach? Do we need to duplicate the Ukrainian approach? Like, for example, what is it, the IT army? I was thinking, how would you even do that in the U.S.?

Mr. Joyce: Yeah. I have never been a fan of, you know, empowering the hacktivists, right, the cyber letters of marque and reprisal that people have talked about. You know, I really believe that nation-state actions are the sole responsibility of those sovereign nations, right, and they have to be accountable for them. And if you’re going to be accountable, you can’t have somebody making up the rules.
Dr. Lewis: I should remind people that if you have a question either hold up your hand and we'll get you a card or, if you're online, there's a button you can click to submit a question and we'll take care of that.

What about some of the other things the Ukrainians did? Like, they benefited from having a lot of outside advice that – we were – we were the people giving the advice in many cases.

Mr. Joyce: Yeah.

Dr. Lewis: What have we learned?

Mr. Joyce: So there’s a lot of lessons to learn from how the Ukrainians protected themselves. So they were – back to that resiliency word, they were very resilient. How did they get that? They got there because they’ve practiced for years, right? They were – they were under the threat of NotPetya and, you know, electric-grid attacks and other things, so they’ve been improving their tradecraft. They’ve gotten to the point where, you know, the Ukrainian sysadmins knew they had to have backups. And when they got a wiper virus, they shrugged their shoulder, they cleaned the machine, they reloaded from backup, and they moved on.

But what they did at the time around the invasion was they got an uplift from U.S. government providing resources, but a lot of pro bono industry support to make them a much harder target. How did they do that? Mostly by getting out of the datacenters in Ukraine that were going to have crappy power and crappy comms just from the kinetic fight that’s going on, and they got up into the Western cloud. And then the benefit of being in the cloud was you now went from two people who were maintaining and operating those servers to teams of hundreds or thousands who had the threat intelligence of: This server got actioned; I need to defend the same thing over here. You got the benefit of NSA working with those companies to take the Russian threats from foreign intel and injecting that in, right? I wasn’t going to find those two server admins in Ukraine and be able to help them directly like that, but that cloud environment gave them a much more resilient space.

Dr. Lewis: Where would you put the U.S. government when it comes to cloud? I mean, there’s some indications that some civilian agencies are actually backing away from the cloud. I mean, do we need to do more to secure it? What’s the –

Mr. Joyce: You know, I really believe the path of the future is in the cloud. So there is – there’s a wide array of people who are doing it right and people who are not doing it right. And it’s just like, you know, managing the server on the ground. It takes effort and knowledge and attention and resources. And I think we are now getting better at specifying the defaults, the things that
rigorously need to be tuned and configured and set. But, yeah, there are still breaches and issues with the way the U.S. government's running cloud.

Dr. Lewis: What would you do to change that? I mean, I'm not asking you to critique FedRAMP, which – what is it, 4,000 pages? What would you do to make it easier for people to use good cloud?

Mr. Joyce: Well, the first thing I would do is you need to decide how sensitive the application is because there's different – there's different integrity levels across the offerings you can choose. And you know, if it has a high regret factor, it shouldn't be a IL1 cloud instance; it should be something much more protected and secure.

Dr. Lewis: Questions? Let me get some questions. Do we have online? Oh, we do. Goodness. Thank you.

Maybe turning before we get to the questions to China, what does a more aggressive China mean for cybersecurity? It's hard to believe they could be more aggressive, but I – are they maxed out? What does China mean for it?

Mr. Joyce: They're not maxed out. You know, the threat of China is capacity and resources. And, you know, we're used to kind of a narrative of this unsophisticated loud threat. And, yes, there is an enormous amount of unsophisticated loud Chinese threat. But there are also elite units that have tools and tradecraft that is very sophisticated.

And, you know, one of the dangers are that knowledge and tradecraft propagating to the scale that they can bring. And so that's the concern as they're able to scale and use that elite set of concept and tools at a much bigger pace.

Dr. Lewis: What would you say to companies when they look at Ukraine and then they look at Taiwan?

Mr. Joyce: Yeah. So we had a lot of companies who had to endure hard decisions and take rapid action at the time of the invasion. And often they had people in Ukraine that were now going to be in a war zone and they had to think about getting them out. They had Russian or Ukrainian CIS admins and they had to think about what privileges they wanted them to have. They had network segments in Russia or Ukraine and they had to think about whether they severed that or firewalled it. They had to think about whether they just pulled all the way out of their Russian businesses and what the implications were.

So what I would encourage anybody who went through that to sit and do a tabletop with your executives; maybe even have your board observe. But
think about if you scratched out Russia-Ukraine and wrote China-Taiwan, how that changes and how much more intertwined and difficult that is, because I think that’s a really hard problem. And you don’t want to be starting that planning the week before an invasion, when you’re starting to see the White House saying it’s coming, right? You want to be doing that now and buying down your risk and making those decisions in advance. And it’s really hard. So tabletop it and see where your pain points are.

Dr. Lewis: That touches on something, though, that was, I think, one of the lessons of Ukraine is the release of what would have been secret intelligence on Russian intentions and motives turned out to be very successful politically. So what did you learn from that? I know sometimes agencies are reluctant to release stuff, but –

Mr. Joyce: Yeah, I think that’s in line with, you know, our overall journey here where, you know, the idea is intelligence has to serve the people who can make use of it. And sometimes that sensitive intelligence is serving the president, the warfighters, the diplomats, the policymakers. But other times, you know, it serves the international community, businesses and others.

So I think you’re always going to find, you know, the policymakers now thinking about that risk-reward, sources and methods, versus the operational outcomes.

Dr. Lewis: Well, as usual, I asked for questions and I got them. So we have – we’re going to be right up to the time limit here. This is a good one, though. It’s my favorite so far. If you woke up tomorrow and you were the director of CISA and Jen Easterly was the director of NSA, would you have a different perspective on things like the joint collaborative environment?

Mr. Joyce: No, I don’t think I would, right. I think the – if you look – I talked about going back to some of the authorities and constituencies, right. The JCDC and the CISA mission has got to be broad. It’s massive and inclusive. And there are things where we can get the NSA’s secret sauce into that world, but also, you know, directly into the people who can do something about it in the telcos, the ISPs, the major equipment manufacturers and the incident responders.

Dr. Lewis: What do you like best about JC –

Mr. Joyce: JC –

Dr. Lewis: The collaborative –

Mr. Joyce: JCDC.

Dr. Lewis: Oh. No, it’s – yeah, JCDC.
Mr. Joyce: Yeah. The JCDC – the best thing – you look at Log4j and it was a phenomenal response, right? There was a place that was the center of the universe for everybody who wanted to contribute to come, bring their knowledge together, share that, and then get it back out to all the interested parties. You know, what software was vulnerable? What is the latest workaround for some of the mitigations people were proposing? You know, it was just a definitive place to go on a very fast-moving process and, you know, everybody brought their knowledge, whether it was government or industry, to that centralized place.

Dr. Lewis: Do you think that’s scalable, though? I mean, maybe you don’t see it. Is it only for the big incidents or what?

Mr. Joyce: Well, that’s – the big incident use case is one of the use cases, right, and so there’s other use cases and I’ll let CISA talk to, you know, where they’re headed with that. But, you know, we’re along and embedded in part of that.

Dr. Lewis: Great. We’re seeing a trend globally towards increasing – increasingly robust data privacy laws, which are often linked to cybersecurity standards requiring data localization. It’s a great question.

How do these affect our global collective defense in cyberspace?

Mr. Joyce: Yeah. I’ll go back to GDPR. You know, there were second order effects that we didn’t – I won’t say we didn’t appreciate because there were people sounding the alarm. They were not fully considered in the weight of that. So, for example, the internet registries where you have to, you know, have accountability of who owns a domain name. Instantly under GDPR the default was you couldn’t know that thing and so cybersecurity researchers all over the world lost the ability to follow connectivity between bad domains.

So we’ve got to think about second order reflections. There is a need for data privacy but we’ve got to have rational connectivity to the rule of law processes that still make cybersecurity effective.

Dr. Lewis: You know, I think if I was going to give – handicap this, I’d say that GDPR is becoming the global standard. We just have to accept that. That the data localization will be tough because there’s a split within Europe on that. But, in general, my impression is that things are better. We’re in a much more cooperative environment than we were, say, two or three years ago. So I guess things like GCC got some credit.

Mr. Joyce: Yeah, and I think we’re learning to work in it. But it’s still – you know, it can be improved, right? I can tell you that, you know, I want the years of my life
back clicking cookie warnings because they are adding no value, right? So we've got to think about the balance in that space. There's rational security and there's some theater in it.

Dr. Lewis: Yeah, cookies. Hmm.

Post SolarWinds General Nakasone said NSA had a blind spot where hackers used U.S. cloud services. Has the new KYC “know your customer” executive order changed that?

Mr. Joyce: I don't know that that has changed it significantly. It certainly has other benefits but not for us in the intelligence world. What has moved the needle is those relationships with the companies, right?

So the blind spot of, you know, that domestic infrastructure the companies know what's going on in their networks and by them pursuing a threat I can tell them about now you don't have NSA feeling like we need to chase that data because it's covered by some really expert analysis, and then they can bring the results back out and we can meet and continue to add that to the foreign threat.

Dr. Lewis: This is a great – we got a lot of great questions but this is a little off topic. I should be doing them in sequence. But where can we trust AI for NSA missions and where can we not?

Mr. Joyce: That's a good question. You know, I don't know how many of you have played with, you know, several of the different – name your favorite model out there. But they hallucinate – and that's the technical term of art – meaning they will generate data that's not real.

I have to be able to generate real data to bring into a company or the president or the warfighters so I have to get to the point where we're understanding that outputs are factually accurate in my world. That's a high bar.

The idea that it will sort and provide acceleration just like I talked about the advantage to the adversary, you know, every single day our analysts are overwhelmed with, you know, what they have to focus on. If it can raise things up, and even if it's only 90 percent right on the things it surfaces, then the human can work in a much more enriched flow. And at that point, they become more effective. So I think that's the place, is the sweet spot in the near term.

Dr. Lewis: So it's a tool.

Mr. Joyce: It's a tool. It's not going to replace our analysts, definitely.
Dr. Lewis: Yeah. I, to prepare for AI, watched “Terminator 3” again, but I didn’t mind that much. So another AI question. It’s the flavor du jour. How concerned is NSA about IP theft targeting U.S. AI leaders, like open AI? Have you seen an uptick in that?

Mr. Joyce: Yeah. So I can't talk to any specific threats, but I can talk with a historic lens, right? All of our industrial advancements that are game changing have been targeted in the past, right? Whether it’s material science or chemicals or battery technology. I don’t care what it is. If we have innovated it and have the state of the art, you know, it’s been under pressure from China and others to pull that and steal and bypass the investments our companies are making to develop it. And so I see no reason that there’s not a major focus on getting those models and bypassing all the investment and, you know, the capital it took to develop them.

Dr. Lewis: Where would you rank the Chinese on things like quantum and AI? Quantum, I got to meet the guy who was the head of the Micius program, and I thought he was the real deal.

Mr. Joyce: Yeah. If you read the open China strategies – and they're – you know, they're – if nothing else, they're strategic and try to align on a vision and a goal in the long term – they're investing in both areas heavily. And, you know, again, the quantity of researchers applied, they're going to get good at it. But they're also going to use that intel capability both in the HUMINT world and in the cyber world to try to jumpstart where we have leads.

Dr. Lewis: This is what I've been wondering about myself, and so it's a good question. It's from people at MIT. Can you tell us how the Vulnerabilities Equities Process is working these days? I could not answer this question.

Mr. Joyce: Yep. So it is still a robust and viable process. For those of you that don’t know, Vulnerabilities Equity Process was set up a number of years ago and refined four-ish years ago. But it’s the process where the government takes a vulnerability it knows about in the cyber area, and considers whether it needs to be closed for the defensive greater good or reserved for the intelligence or warfighting capabilities. The default on this is overwhelmingly default to defense, but the retention of some of those capabilities are necessary for the cybersecurity intelligence I produce, for some of the activities to do the defend forward mission.

So but it’s still active. It involves the intel community, but it also involves – you can go out and see the charter – it involves DHS, CISA. It involves folks in Commerce. So there’s a wide array of voices around the table.

Dr. Lewis: Yeah, no, it’s good to hear it’s still working. It’s not always visible. What does
– and I’ll just read it. What does NSA do in the case of obstinance when you have a private actor? Especially if there’s a vulnerability in a handset or one of the drivers from the handset? And they refer to a particular company. And the company’s – the supplier is unwilling or unable to handle, and the handset is used by a lot of people. What can NSA do about that?

Mr. Joyce: Yeah. So that – we just talked about the Vulnerability Equity Process. That’s been one of my frustrations, is when you have a vulnerability, it’s clear it needs to be fixed, and you go to a company and either they’ve decided the product’s end of life or that it’s – you know, it’s a feature not a bug. We’ve been told that before. But, you know, the idea that it’s not going to get fixed. That’s a hard problem, right, because we can’t mandate the cybersecurity there.

We will often at that point do responsible disclosure. The good news is it doesn’t happen much. But the idea that, you know, you’ve got to find a way to increase the pressure to get it fixed, because you can’t go directly public and make that vulnerability known if the company has no intentions to fix it. At that point, you’ve just armed the bad actors with that knowledge as well. So it’s a tough problem. But usually we use the levers of government to bring increasing pressure.

Dr. Lewis: Maybe related to that, as 5G brings ubiquitous connectivity with big data, and AI, and cyber, what can the U.S. and its allies do to ensure that places like China don’t establish tech dominance? I’d say it’s a tossup right now. We were – we were doing better. The Chinese have kind of regrouped and are moving out faster than we might want. But what would you think we could do?

Mr. Joyce: Yeah. I think the thing we need to do is really shine a light on the values and the outcomes you can expect from the different – the different governances, right? I think we’ve bought into cheap technology, and that has fueled the growth of China. You know, whether you look at Huawei or other technology, we are starting to realize that we’ve got to turn and make sure that in the West, we can produce and deliver secure things – CHIPS Act, you know, the Open RAN concept. You’re going to see more things to intentionally ensure that we have a secure supply chain that we can turn to, and make the choice to buy secure, use secure.

Dr. Lewis: One of the things you got – our last question will be about TikTok, but I’ll cheat and slip one in now. One of the things you hear from people is, well, there’s no evidence that they’re doing bad things. And I believe that could be true. But what would you say back to that, to you don’t like risk?

Mr. Joyce: Yeah. I’ll give the quotes I always use, right, which is this is not about show me the smoking gun; this is, the adversary has a loaded gun. You know, why
would you stand in front of that, right? You’ve given them the platform and the capability to do harm. And you know, if, given the historical track record of how they operate with their businesses, how they choose to exploit the West, it’s an untenable situation.

You know, the idea that TikTok as a platform – you know, do I think if I loaded TikTok on my phone, they’re going to get to all of the other sensitive things through that TikTok app tomorrow? Probably not, right? The cost of exposing TikTok in that way to exploit one or a small set of users probably isn’t worth it. But all the data, the metadata that they collect, that goes back to big servers accessible to China, that’s a problem.

The idea that they own the algorithms that promote or suppress the content, that’s a huge problem, when you have millions upon millions of eyes consuming the content, and they can dial up something that is divisive, or they can dial down something that is threatening to the PRC. That’s the advantage, right? That is – you know, the analogy I used is, we’re bringing that Trojan horse inside the castle, right? Why would you, knowing what it is, bring it into the castle?

Dr. Lewis: A couple more questions, and this one’s still the China theme. With China’s quantum leap in January, do you think NSA’s plans to move to post-quantum encryption by 2035 still make sense? Does that development speed up the timeline?

Mr. Joyce: So I’m unclear what they mean, China’s quantum leap. There was a discredited plan out there, and it was not valid, that there was a – there was a shortcut –

Dr. Lewis: I think that’s what they mean.

Mr. Joyce: – to quantum. Yeah, so it wasn’t a quantum leap, so we’re still comfortable with our timelines.

Dr. Lewis: Okay.

Mr. Joyce: And, you know, it’s – quantum – the quantum threat is not here yet. But you can see it on the horizon. So you need to be doing prudent things to get ready, and that’s, you know, the newest competition, to give us the crowdsourced solutions for quantum-resistant algorithms. Many eyes vetted and tested, to include NSA, the commercial entities who are now operationally testing those things, to understand what it does to the infrastructure, and the requirements to host those new types of algorithms, and optimize for them.

And then, you know, thinking about what’s your inventory. This is a Y2K-like problem. Where do you use public key cryptography in your infrastructure?
And what’s your plan to kind of wash it out on those same orders, right? You ought to – you ought to look at where the government’s heading and say I need to be there in the same timeframes.

Dr. Lewis: I will say that the timeline for Quantum is one of the few places where I think you could get technological surprise, because if they did have that capability they wouldn't have advertised it. You don't want to wake up and find out that they've got it. And it’s a real – and you also – one of our colleagues from the early days of cybersecurity is now talking about Y2Q. So stay tuned for that one.

OK, I think it’s the next to final or the final question. What can NSA, CISA and FBI do to protect small companies?

Mr. Joyce: I told you where NSA is, right? Our strategy that gets to scale is to get to the bigs in the ecosystem that can then push that security into the ecosystem, right. Even in the DOD, the numbers are staggering. So I mentioned we've got about 300 companies that we’re interacting with. There is something like 30,000 cleared defense contractors. Those are people that have access to classified material, doing work and development for the Defense Department. So 300 to 30,000, that's a big gap. But there’s 300,000 defense contractors. Now, they make all sorts of widgets, but they’re in the supply chain. And disruption of that supply chain would be a heinous thing.

So we are not scaling to get to 30,000, let alone 300,000. We’re using that strategy to get to the big companies in the ecosystem and do those things like, you know, the defend-forward strategies and others to disrupt the threats. And by doing that, it not only protects the 30,000, the 300,000, but it gets into the critical infrastructure, the business, our foreign partners, and the ecosystem.

Dr. Lewis: So for those of you who have a doctorate, this is a lot what you Ph.D. oral exam is like. You have a bunch of grumpy professors who get to throw any question they want in the general area at them.

And would you give Rob a passing mark? I think yes. So an A, they say. That’s impressive.

Mr. Joyce: Thank you.

Dr. Lewis: Any final questions? If not, Rob, thank you for taking the time.

Mr. Joyce: Thanks, Jim. I appreciate you listening.

Dr. Lewis: Thanks. (Applause.)