Center for Strategic and International Studies

TRANSCRIPT

Online Event

"The Future of Quantum – Driving Innovation and Security from the Government"

DATE

Monday, May 16, 2022 at 3:00 p.m. ET

FEATURING

Jonah Force Hill

Director, Cybersecurity and Emerging Technology Policy, National Security Council

Charles Tahan

Assistant Director for Quantum Information Science and the Director of the National Quantum Coordination Office, Office of Science and Technology Policy (OSTP)

CSIS EXPERTS

James Andrew Lewis

Senior Vice President and Director, Strategic Technologies Program, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

James Andrew Lewis: Good afternoon. Welcome to CSIS. My name is Jim Lewis. We're having an event today in "The Future of Quantum." It's part of our series on quantum computing. We're talking about driving innovation and security from the federal government. We are lucky today to have two excellent speakers – Jonah Force Hill, who's the director of cybersecurity and emerging technology policy at the National Security Council and Charles Tahan, who is the assistant director for quantum information science and the director of the National Quantum Coordination Office in the Office of Science and Technology Policy.

So we're going to talk about some recent announcements by the White House, what the future of federal policy will be when it comes to quantum, and what our guests think the next few steps will be. So with that, I've asked them each to speak. And we will turn it over to Jonah to start.

Jonah Force Hill: All right. Thanks, Jim. Thanks for having us here. So I assume folks who've gone to the link have seen that we released – on May 4th the president signed two presidential directives on quantum science and technology. The first was an executive order that enhanced the National Quantum Initiatives Advisory Committee. This essentially was raising the prominence within the U.S. government of the advisory committee within the National Quantum Initiative, moving it from the Department of Energy to the White House under the Office of Science and Technology Policy.

And the second, released on the same day, is a national security memorandum, which is essentially an executive order for national security issues, that's focused on promoting U.S. leadership in quantum computing, while mitigating the risks to vulnerable cryptographic systems. So it's a bit of a mouthful of a title. It's the 10th national security memorandum issued by the president. So it's titled – or, numbered NSM 10. And the title, while it's a little long, does do a good job of describing the objectives of the directive. And together, I think the executive order and national security memorandum articulate the administration's position towards quantum science and tech in a pretty clear and forward-looking way.

At its core, the policy is that this is a technology that poses both – or, raises tremendous opportunities for science, technology, engineering, but also carries significant risks primarily to the cryptographic systems that are used to secure a variety of digital systems on the internet and in technology generally, so specifically public key cryptography in various forms. So what the NSM does is lays out a series of actions for departments and agencies across the U.S. government to both promote and mitigate the risks of quantum technologies, particularly quantum computing.

So quantum, as Charlie will describe at length, isn't just quantum computing. That's the application that most of the public is aware of, but there are a variety of other applications of quantum information science that similarly pose risks, but also present tremendous opportunities for the United States and the world.

So I'm happy to walk through all the various pieces of the NSM, but really what it does is it gets us started on a multiyear process to migrate to systems of cryptography that are secure or more secure than the ones we have now that will be resistant to attacks by quantum computers when they reach the requisite level of sophistication and processing power.

Dr. Lewis: Great. Thank you.

Charlie, over to you.

Charles Tahan: Well, thanks again for having me and, Jonah, for that great introduction to the NSM. Maybe I'll just take a step back. Quantum may be a critical and emerging technology but it's not new. No, the government has been significantly funding quantum information science research for 25 years and we've gotten to a point where we're starting to see the first examples of applications, you know, that could benefit our society.

Three years ago, almost four years ago now, Congress passed the National Quantum Initiative Act which created my office. It created quantum research centers across the country. It called for an advisory committee, which we just launched for this administration, and a number of other items. And maybe most important, it asked the agencies across the government to develop a coherent strategy. You know, if I had to summarize that strategy it would be, get the science right, enhance American competitiveness, and enable our people to benefit from this new field as it grows.

So the NSM that Jonah mentioned – the National Security Memorandum – really gets to the heart of this balance between the opportunity of this new technology as it manifests itself and the potential for it to cause harm. And we kind of break out the different technologies of quantum; it's sensing, networking, and computing. Computing in particular, you know, has a potential for true disruption. We know and we knew back in 1994 that for certain problems a quantum computer could be exponentially faster than a classical computer, so, for example, breaking public-key encryption, a classical computer, the biggest one you could imagine, might take a billion years to solve – (laughs) – that problem, whereas a quantum computer, the estimates are pretty divergent, but it could be a month, it could be a year – exponentially faster.

So you really have to, when you're thinking about cryptography, about protecting information like medical records, financial records, the president's communications, information that you want to protect for 25 years or more, you have to be extremely conservative. And we know that moving to a new cryptographic system can take 10 years or more, if you do it right. You know, so you really have to be forward leaning in moving the nation and, indeed, the whole world to algorithms that are protected against future quantum computers. Maybe I'll stop there.

Dr. Lewis: Great. Thank you. So what did the administration want from the EO and the NSM? Why issue them now? And I'll ask that to both of you.

Mr. Hill: I'll start at least on the NSM. You know, I think this is an area that, you know, is widely supported across the aisle in a real bipartisan way. It's sort of a no-brainer that the U.S. government and, by extension, critical infrastructure, the financial sector, critical industries across the nation need to start now, as soon as possible, preparing for this future in which public-key crypto is vulnerable to a quantum computer. We know that there is a very high likelihood that we will get there in the next 10, 20 years, and as Charlie mentioned, the time it takes to plan, to budget, to set benchmarks to integrate new cryptographic standards takes a very long time. You know, some industries will be very quick to adopt, some technology companies and other industries with resources are already starting to explore what they need to do to effectively make the migration. But there are a lot of sectors and areas of the U.S. economy that aren't going to be equipped to do this quickly and won't be able to make the kinds of necessary migrations alone.

So getting the U.S. government coordinated to help those parts of the economy and those parts of the country that really need that assistance, I think this is something that was widely understood across the administration and on both sides of the aisle as something that was a priority to get moving on.

Dr. Tahan: I'll just add to what Jonah said. The national – the executive order on the NQIAC – the National Quantum Initiative Advisory Committee – is really this administration's statement that the NQI continues to be a national priority.

You know, it makes it clear that all the agencies participating in R&D funding of quantum need to work together. It makes it clear the advisory committee advises the president and the director of OSTP, so that's the intention of that EO.

The second part of the NSM – I think there's two really important things to remember if you don't remember anything else.

You know, the first one is, in order to protect yourself against a future quantum computer, you don't need quantum technology now. You know, we know how to protect our networks with classical protocols that are already very near complete, and so, we can act right now to protect our networks. And because it takes a long time, we need to do that.

The second part is, in order to ensure that the government really moves quickly, there needs to be presidential direction for the agencies to budget, plan for this equitable transition, as Jonah said, and coordinate, you know, what systems are vulnerable so that we can ensure that, you know, within 10 years or 15 years we're done. You know, and that really requires high-level coordination.

So, that was – those are the goals, in my opinion, of the two documents.

Dr. Lewis: So, the way I was thinking about this is you've got one piece on risk, one piece on opportunity, and it would be cheap to assign each of the speakers one of those because they actually do both. But this is CSIS, so let's get it out of the way. Did you look in the rearview mirror when you were thinking of these?

Dr. Tahan: Well, let me – let me – you bring out a pet peeve here –

Dr. Lewis: Uh-oh.

Dr. Tahan: – because the NSM actually is not just about protect. It's got three components.

You know, the first one – and we intentionally made it first – is the "promote" piece, right? You know, this is a commitment to not slow down the commercialization of this technology, our scientific benefits of this technology, our workforce development, but instead speed it up. So number one of the NSM is speed it up – you know, speed this technology up.

But at the same time, number two is, while we're doing that, protect our networks as fast as possible. And number three is also critical, which is this balancing of we want to move our science industry forward as quickly as possible, but we need to do that in a careful way because we have this gap, where it's going to take time to protect ourselves, and we don't want our information being stolen and used against us.

And we don't want the negative consequences of this technology to be – you know, to go to bad actors. So, it's critical – the NSM has three parts to it, you know, and two of them are really focused around moving faster.

Dr. Lewis: Yeah, that's probably the right approach.

Did you want to add anything to that, Jonah?

Mr. Hill: Yeah, just, you know, the NSM even though it is a National Security Memorandum, like Charlie said, is focused on promoting foundational science and workforce and educational programs, right? To have the national security issues addressed, which are decades-long issues, we need to create an environment domestically that can adapt and respond to those threats as they emerge.

And you need well-trained physicists, mathematicians, cryptographers ready to meet those challenges in 10, 20 and 30 years in the future.

Dr. Lewis: So, one of the questions we always ask here is, how are we doing compared to everyone else if you were going to list off the top of your head? And of course, there's some country that begins with the letter c that everyone thinks about.

How are we doing compared to everyone else when it comes to quantum, both in securing ourselves and in creating the research that will bring opportunity in the future?

Dr. Tahan: I can take that. You know, the one thing I like to say – and it's actually very clear also in the NSM when it mentions the importance of cooperating with our international allies – is that quantum is a global endeavor. It has been, you know, since always. You know, many of the founders of quantum mechanics, who were originally from Europe – I mean, Bohr, Eisenberg, Einstein – even into the 1980s some of the original proposals of quantum computing came from England, for example.

So, it's always been a global endeavor. It's critical, you know, to science and finding applications of this technology. You know, so it's still – the reason we call it a critical emerging technology is because we don't have all the answers, right? You know, we are still trying to understand the applications for a large-scale quantum computer, or a small-scale quantum computer. We're still trying to understand how sensors can enable new biomedical imaging, for example. So there's a lot of discovery to be had, and the last thing you want to do when you're trying to discover new things is to close yourself off. You want to work with other people and pursue the fundamental questions. So that's number one.

And in terms of how we're doing, the U.S. is certainly a leader in quantum information science, both in the development of hardware in theory and in developing cryptographic protocols. But we do it in this global context. So, for example, NIST, the National Institute of Standards and Technology, they

are running a program – sort of a competition between, you know, different types of protocol suites. And each of these teams are made up from expert cryptographers from all over the place. You know, and really – you know, the whole point of making good cryptography is beating on it as much as you can. (Laughs.) So finding smart people to try to break it. And so the more hours you can get of smart people trying to break it, the better your cryptography is going to last. So, you know, in many of those respects it's really about how can we help lead the world to finding good applications while protecting ourselves?

Mr. Hill: Yeah. I'll just add, you know, I think the United States is in a generally favorable position vis-à-vis China in this area because of the collaborative nature of American science and industry, right? You know, Charlie can speak about the number of partnerships that this administration has formed with our partners and allies on quantum information, science, R&D, and information sharing, and academic exchanges. You know, China is – you know, they do not have that same sort of broad coalition working together that we do. So I think that's a huge competitive advantage.

And just sort of the freedom to engage in scientific endeavors in the United States really is unparalleled. Our universities are unmatched and, you know, I think we're going to continue to maintain an advantage, so long as we continue to invest in the kinds of things that we need to invest in, both in R&D but also, again, in the basic science that can really, you know, drive new innovations in this set.

Dr. Lewis: I want to focus eventually on the opportunity part of this equation, but maybe one more question on risk – well, maybe two. Part of – one of the documents, it might have been the NSM; it might have been the EO, said you wanted to educate people on the threats that they were facing. What's the reception been? What's the message? I mean, what does educate on the threats mean? I mean, are you talking to bankers? Are you talking to grocery stores?

Mr. Hill: Yeah, so there are a few things. The NSM does direct federal law enforcement agencies in particular to, like you said, educate those industries and labs and others that are engaged in R&D and science on quantum information science and tech, so that they realize that this is a – you know, a technology area that is ripe for abuse and manipulation and theft, right? We know over the last 20 years China has been quite aggressive on intellectual property theft. And a lot of these companies that are working in this field may not be aware of the specific risks that they face and may not be employing the most up-to-date cybersecurity best practices and defensive measures that they need to be taking.

So just getting the word out there. When we have just, you know, concrete threats, you know, indicators of compromise that we can share with those companies we will do that. It's really about making sure that the companies that are working in this space are not ignorant of the risks that they face just participating in this industry. And so that will get more sophisticated as time goes on but, you know, we're going to try to build those relationships now so that, over time, those companies can build up their resilience and their capability to defend themselves.

Dr. Tahan: I'll just add that a key part of the NSM is also asking the agencies to educate each other. You know, so depending on who you ask about quantum, you might get an answer that is still very much science, right, and a lot of – and that's true to a certain extent. But at the same time, we do live in this much more competitive world. And when you talk about building, you know, very advanced quantum computers or other types of technologies, it's not the same thing as building LIGO – you know, the gravity wave detector – or a particle accelerator because there are these economic and national security implications. So you cannot treat it just like a science experiment; it really is something that has a dual use potential.

And so when you're developing R&D programs or acquisition strategies or user access to these machines, you really need to think carefully about, number one, don't slow it down, but how do you ensure that you're not being taken advantage of. And that's really, you know, part of – a bit of part of what the NSM is about, is trying to educate across the government and with industry and the big national labs, you know, how are we collectively thinking smart about this new technology.

Dr. Lewis: So our last event we had some really great scientists – it was an all-science panel – and they said maybe 10, maybe more years out before we get this. And it made me think that one of the things that people used to talk about was technological surprise. So, you know, it would be a surprise if we found out that other people could read things that we thought were encrypted. What are the indicators that you'd look for to say somebody else is pulling ahead in quantum or is taking advantage of quantum? I don't know if you've given any thought to that, but what would be the indicators and warnings for technological surprise in this field?

Dr. Tahan: Well, remember when I said that the government has been funding this for 25 years, you know? And this is a good example of why, you know. Back in '93 – so quantum computers were proposed in the '80s, you know, like toy models. Then, in 1993, Peter Shor, then at AT&T, came up with Shor's quantum algorithm, which is for factoring prime numbers exponentially faster, which would break a particular type of encryption that we use in public key cryptography. So immediately the government said, well – (laughs) – you know, this might be crazy, but we need to make sure. You

know, we need to understand it. And that fueled a lot of basic research at various agencies – DARPA, IARPA, across the DOD – to understand, like: One, is it physically possible to make these machines? Two, you know, when, if ever, they could actually be built. So there's a tremendous amount of history and experience built up within the government about how fast have things been developing.

You know, and again, where you – where you look now in the industry – we're at around 50 qubits in quantum computers – you can tie that back to the 20, 25 years of development that's been funded over – you know, and many of the same researchers were funded as students, postdocs, and now in industry. Those are coming from government programs. So there's a lot of experience, and so far we haven't seen surprises like that.

They've been – you know, there's been a maturing of the technology, hard fought because this is a tremendously difficult problem, you know, to build a large-scale quantum computer. It's sort of like going against what the universe wants you to do. (Laughs.) The universe doesn't like quantum states to be that good. It's been a hard-fought slog to make all the different components of a quantum computer better.

So I think we have those indicators, but it's something you need to watch. You know, there can always be breakthroughs in mathematics and cryptography and the physical devices.

Dr. Lewis: Jonah, I know there's bits of the documents that didn't – weren't made public, but what did they talk about in terms of surprises? Staying up late at night worrying about this, what do you look at? What are the indicators you look at?

Mr. Hill: So, yes, there are parts that cover sensitive national security issues, so I can't really speak about those.

Dr. Lewis: Really? (Laughter.)

Mr. Hill: You know, I think it's pretty clear that, you know, advances in the field are generally out in the open. You know, there are, obviously, programs that were – that are more closely – more closely protected. But you know, I think as a community we can see where the technology is going and how advanced and how quickly it's moving. I, you know, defer to Charlie and the experts on the physics, but you know, the number of qubits and the processing power of quantum computers, at least, you know, isn't – doesn't seem, at least, to be moving at a speed that we can't easily track and anticipate. Yes, there could be some surprise, but if you follow what the leading companies are doing, what the national labs are doing – which, you know, are eagerly putting their achievements out to the public – you know, we're some time away. That

doesn't mean, again, that some new innovation could radically speed up the process, but for now I think, you know, it's a more gradual, incremental advancement, like Charlie mentioned.

Dr. Lewis: So one of the questions I was going to ask is: How do we do better at collaborating with academic research and the private sector? But Charlie, if it's been going on for 25 years, where do we need to improve? Or is it really fine?

Dr. Tahan: Oh, yeah, there's always room to improve. (Laughs.)

Dr. Lewis: Of course. Yeah.

Dr. Tahan: You know, a big part of the NSM – you know, why is the NSM public? You know, we very deliberately made that intention.

One, because the nation as a whole has to move to post-quantum cryptography. So that's got to be a national priority.

The second part is we want input from industry. You know, traditionally, if you look back the last 50, 60, 70 years, how does the government protect technology? It's our export controls, classification. You know, these are very blunt instruments that can slow down our industry, that can hurt our long-term economic prosperity – they can slow down the science in this respect. So a big part of our public engagements and the reason to put this in the NSM is just to ask industry: Do you have a better idea? Like, what are you doing to protect this by improving cybersecurity, by, you know, developing user-access protocols? You know, what are the creative ideas to help us move faster while protecting it? So – and that's one example. There are many others, but I think that's a good one.

Dr. Lewis: Did you want to add anything, Jonah? Oh, OK.

Well, then, another thing that we've routinely found in this series of events is that most of the work that's making progress – a lot of the work that's making progress is outside the government and most of the spending is outside the government. So what kind of collaboration problem does that pose for you? I mean, some of them are research facilities that depend a lot on the government. Others are giant companies that don't. So how do you pull all that together? What's the best way? Because it won't be – you know, there was a model in the last century at this point in the last century where DOD led on a lot of research; not true anymore. So it's a really different kind of path to go down.

Dr. Tahan: Why don't you take the crypto piece?

Mr. Hill: Yeah.

Dr. Tahan: I'll take the science piece.

Mr. Hill: OK. In what sense, the crypto piece?

Dr. Tahan: Well, how do you work with companies to convince them to move?

Dr. Lewis: And which kind of companies? Is it crypto companies? Is it financial companies? Is it – who are you working with?

Mr. Hill: Yeah. I mean, so, for starters, we are waiting on NIST to release their initial set of standards. You know, creating awareness within industry that these are coming and that they need to prepare and start inventorying their cryptographic systems internally to start putting in place the kinds of what we call cryptographic agility in the way that they design their systems, so that you can easily plug and play those new standards when they are finally released.

So, really, we're working with everyone on this, starting with the U.S. government itself, to get our own house in order before, you know, we start pushing for industry to do the same. But you know, it is – like I said earlier, industry is at different levels of sophistication in this stuff. You know, the financial institutions, the organizations with resources are going to be able to adopt rather quickly. The ones that have more legacy systems, that are more difficult to update, that already have outdated forms of encryption baked in, those are going to be more challenging.

So, on the crypto side, you know, it's a fundamentally different problem than the collaborative issues on the science and tech on quantum computers and quantum information science generally. But you know, as the science and the engineering evolve, we need a commitment from industry to move forward at the same pace.

Dr. Tahan: Yeah. I'll just say, you're absolutely right that funding in quantum tech on the industry side has dramatically increased. You know, five years ago you really couldn't say that. And in fact, we had an event at the White House this fall where we brought in many of the leading quantum computing companies and quantum sensing companies to talk about, you know, how do we work together in the future?

And I think there's a few things, you know, where the government still plays a critical role that the companies really need. You know, one, we still do invest a lot in R&D, which will be critical to their future developments. What you're seeing now is a lot of the companies integrating human technologies that have been developed over a long period of time to bigger systems, but then what happens to the next phase, and the next phase, you know? So there's a lot of arguing to do.

The other thing is, of course, that government is a great first customer, you know? So when you're building one of these very exotic machines where you don't really know the applications, obviously the companies would love to sell to the government. And so if you want to sell to the government, you know, we can say, well, have you met these criteria? Is your cyber – is your cybersecurity up to snuff, and so on?

I would say the other part is applications. You know, so there still is a bit of a build it and they will come sense of the field. You know, we have a few great applications. Cryptography is one with a – you know, a national security implication. We think chemistry in the long term. But there really is a need to find more applications to make this a going concern. And companies are interested in the government supporting that kind of search. You know, so there's a lot of places where the government can have influence. You know, we're still a free country. We're not going to tell, you know, companies what to do. But, you know, I think in a partnership there's a lot of places where we can – we can benefit each other.

Dr. Lewis: He was going to come back to the – you said early on we need to identify applications that we'll need. And that's the problem in a lot of new technologies. It's a problem in 5G, for example. But one of the issues that's come up in quantum is this idea of quantum as a service. I'm sure you've heard of it. Is that going to be helpful to us? That, you know, you're a researcher. You're not going to have a quantum computer in your facility, but you are going to be able to access it. How important are things like that?

Dr. Tahan: I think it's amazing. You know, in the sense that we already have the cloud, right? You don't have to rebuild the cloud. So you have the cloud, you can add quantum ability as a – as an add-on feature that, you know, physicists can use to try to search for new applications or, you know, proof of concept experiments. It's a tremendous way to do science. I think we will see how far it goes in terms of – unless you find those initial applications to justify it for business use, there's a limit for how much of it is for research. You know, you also want to balance, you know, skewing the market in terms of, you know, doing stuff on it that doesn't make sense, right?

So I think it's awesome. It's amazing. It's a great development. And we're going to hope that over the next few years, as we start to see systems with

hundreds of qubits and more, that people find things that are really dramatically new you can do with them. That's the big question.

Dr. Lewis: So, Jonah, is this a cybersecurity problem that's different from other cybersecurity problems? Or is it just the general –

Mr. Hill: I don't think it's fundamentally different. It's a difference of scale rather than kind. You know, previous migrations of cryptographic standards took a lot of time and a lot of resources. You know, SHA-1 to SHA-2 to SHA-3. You know, from the new AES, right? These standards processes take a lot of time and they're hard to implement. It's not just a, you know, you pull one cryptographic standard out and put in a new one, right? They have different key sizes that require, you know, different load balancing arrangements. It's not a – it may sound easy. All right, we got a new standard, just replace the old standard. But that is incredibly difficult. And like I said before, not all organizations are going to be able to do it at the same pace.

This is different in scale in that the types of cryptography that are vulnerable to a large-scale quantum computer, you know, that's everywhere, right, and it's in systems that you might not expect. You know, organizations often don't even know where the cryptographic standards that they use are within their networks, so even just identifying, you know, this is a vulnerable system and this is a protected system, just determining that internally is going to be a tremendous effort for organizations. So I don't think it's a fundamentally new cybersecurity risk, but it's a pervasive one that everyone needs to be paying attention to and, you know, steadily working towards.

Dr. Lewis: We're starting to get a few questions from the audience, I think. Is it a button on the bottom of the screen that would let you, if you want to submit them, but we do have a few and they're all good, so let me – I had warned Jonah, at least, beforehand that I would screen out any of the bad ones. Haven't had to do that. The first one is great and it fits right on this topic. What are the most important focus areas to enhancing American competitiveness on quantum? How can the government help on this?

Dr. Tahan: Sure, this is a big part of what we think about. I should say, if you're interested in this, we put all of our strategies and events on quantum.gov, you know, so you can go there and read to your heart's content.

One example are these grand, technical challenges. So if you list – if you take any potential application – I want to make a very lightweight brain imager with quantum sensors, I want to make a large quantum computer to do quantum simulations, to do drug design – you can start to list all the problems – (laughs) – all the challenges you have to overcome to face it. We call those the quantum frontiers, and there really are a lot of technical questions that still need to be solved. You know, so what we did is we held a

whole bunch of workshops, we put out a request for information, we collected hundreds of pages of input from the experts across the country, and we narrowed them down to the top 10 hard, technical problems, so that's a focus area for R&D investment that the government agencies can do that can help enable, you know, the R&D. So that's an example.

One more example, and then I'll turn it over to Jonah, is bringing these concepts from lab to market, right, so we have quantum – the Global Positioning System, you know, relies on atomic clocks; they've been developed for 50 years, more, but they're many generations behind. You know, we have clocks in the laboratory that can measure, you know, differences of a second in the age of the universe, so how do you bring those from labs to markets, make them smaller and more compact, more durable, cheaper? That translation, you know, which hopefully will be a part of some DARPA-like programs, the new NSF directorate, you know, that's a critical role that government can help play, especially when the market is uncertain at the beginning.

Mr. Hill: Yeah, I would just add, you know, we still don't quite know what the economics of this is going to look like, right? Is the first-mover advantage in quantum science and tech one that then is self-perpetuating? So, you know, if you are the first to develop a large-scale quantum computer, does that then give you the ability to analyze information that lets you optimize for an even faster, even more powerful, more accurate quantum computer? And so the government can really sort of help by continuing to promote American leadership in this space, such that if we're in an environment where we realize, you know what, the first country or first company to develop quantum computers that can do the kinds of things that we think they can do, you know, ensuring that we are in a position to capitalize on that as a nation.

Dr. Lewis: I'd say quantum supremacy but it would just get me annoying mail from people, so I won't.

Charlie, you mentioned the top 10 hard problems. How many of them can you remember off the top of your head?

Dr. Tahan: Oh, probably – I wrote that two years ago. But, you know, there's quite a few.

Dr. Lewis: (Laughs.) It's not a fair question but I couldn't resist.

Dr. Tahan: How do you make better qubits? Like, the central-ness of quantum is that it's extremely delicate, right? It only manifests itself typically when you make things really small and really cold, and what we're trying to do is make things bigger – (laughs) – and warmer and do more things to them and still

make them quantum. So how do you make quantum systems that are better is a big one.

Another is, what happens when you put multiple – more and more qubits together? You know, companies are putting 50-100 qubits together. Does something happen? Does something break, you know, physics-wise, that prevents you from scaling up? Like, it's a very unusual area. So there's a list of things like that.

And I'll just come back to this – you know, what I said at the beginning, getting the science right. You know, to me that means you focus on the hard problems first. You don't want to lay a whole bunch of cable before you even know how fiber optics work, because very likely you're just going to have to replace the cable. So you want to – you want to solve the hard problems, explore the space enough, and then focus on the stuff that's going to work. You know, you don't want to put all your eggs in one basket too soon. So that's sort of our philosophy.

Dr. Lewis: It's kind of the story of the first transatlantic telegraph cable, 170 years ago, which only worked for a couple months because they hadn't worked out all the details and had to replace the entire thing.

Dr. Tahan: Well, you want some of those, right? You just don't want it to be all of them.

Dr. Lewis: Yeah. Big test.

Dr. Tahan: Yeah. You want some of those.

Dr. Lewis: So next question, also a great one. What are the key points for advancing U.S. workforce on quantum? And we haven't talked about workforce. It's a different set of skills. I know both of you have thought about it.

Dr. Tahan: Yeah, this is a big thing for me. Do you want to start, Jonah?

Mr. Hill: Yeah, sure. You know, I think the NSM succinctly describes the goals here. You know, you want to create an environment where, you know, the workforce of the United States wants to stay here and work in industry and academia and the government. And you want to attract those leading thinkers from abroad to come here, right? The more talent we can have, either through, you know, fostering, you know, kids and young people domestically, and the more people we can bring in from overseas to come and work with us, the better. So it's really identifying the right skillsets, identifying the right expertise, and bringing as many talented people together as you can to work on these hard problems.

Dr. Tahan: Yeah. I mean, to me, I said science is first, but workforce is very close second. And it starts with great careers at the end of the day. You know, that these – if your child goes into quantum, you know, they will do OK. You know, that the skillsets that go into making a big quantum computer or a big sensor system, let's think about it. You know, physics, electrical engineering, mechanical engineering, chip design, microwave circuit design, material science. Even if quantum doesn't pan out, we still have autonomy, AI, microelectronics. You will have a great career. There is – you know, we cannot hire people fast enough right now to meet even our quantum jobs, let alone microelectronics, AI, and autonomy.

So these skillsets, these deep science skillsets, are just tremendously valuable. And our focus has been communicating that message so that people know, you know, this is – this is – there's a pretty good bet, you know, if you're good in any of these that you'll be – you'll be – you'll be quite good. And you'll have not only a good career, but a lot of impact on the future of the country

Dr. Lewis: One of the companies that leads in developing quantum computing let me look at some of the coding needed to take advantage of the quantum computing. It's really different. So what are people going to need to learn? You mentioned physics. You mentioned some of the other things. But beyond physics, just basic coding to take advantage of this. What does that entail? And, Jonah, what does that mean for encryption, when we get there?

Mr. Hill: Do you want to take first or second?

Dr. Tahan: Sure. Here's the thing. You know, when you grew up – you're probably not as good at computing as your kids or your grandkids, right? You know, because when you grow up with something you just – it becomes a part of you. And I really believe that quantum mechanics, you know, we're very used to when you drop a ball, it falls. So we know gravity. We're very comfortable with it. We're not familiar and comfortable with quantum mechanics because we don't experience it in our daily lives, right? So if you can build tools like games or computer environments where people can get familiar with it early and develop quantum intuition, you know, amazing things could happen. (Laughs.)

Things that would – you know, it's just like finding people who are really good at languages just by giving them games and tools to kind of assess and accelerate that capability. So I think really as people – giving people experiences early – curriculum, you know, games, tool sets in high school, people will just grow up with this. And some of the stuff that just seems really hard in quantum mechanics may very well become natural to them. And it's just a matter of practice, you know? And your brain changes over time. I still remember my first, you know, physics professor. (Laughs.) He's

like, your brain will hurt for a year, and then you'll get used to it. And you'll accept it. And you'll learn the rules. And I think that's true. And the earlier you do that, the better and easier it is.

Mr. Hill: Yeah. And on the cybersecurity side, you know, I think in a lot of ways it's a similar progression. You need young people excited about cybersecurity, right, you know? The sexy part of the IT and ICT business is generally – you know, are those cutting-edge applications and new products and services, not how do we secure those products and services, right? So making cyber security a priority in computer science education programs, right? If you ask most computer science undergrads, did you have a security class in your curriculum, they would say no, right?

So getting people excited about cybersecurity, getting young people to realize that the introduction of quantum into the cybersecurity field is actually going to present lots of new exciting opportunities for innovation, you know, not just on the defense side, in terms of defending against a large-scale quantum computer, but actually there will be quantum key distribution and quantum communication networks, and all these other things that can actually provide really new, exciting cybersecurity products that, you know, are going to be cutting edge and they're going to provide you with career opportunities, you know, as long as you're interested in continuing to work on those things.

Dr. Lewis: One of the things we found with other technologies, particularly with some of the AI applications, is gaming turns out to be really important. What would a quantum game look like? What would be different? Is it Dungeons & Dragons, but just on warp speed? (Laughter.)

Dr. Tahan: There's quite a few. Last – just this April we celebrated the first World Quantum Day. And a big part of that that we worked with the universities with was to develop modules that would go into high school classrooms. And so they would go in and teach – and present them a few different games. So for example, quantum chess. Like, chess but with quantum rules for how to kill your opponents, right? And quite quickly people learned the new rules and can learn the key concepts. Quantum mechanics sounds mysterious, but there's only like three or four rules that once you get them makes you much more comfortable. And so there's quantum tic-tac-toe, quantum Flappy Bird – you remember that? (Laughs.) That game for your phone? You know, there's a lot of things, you know, that can teach you these core concepts in a fun way, yeah.

Dr. Lewis: We got a question about what are the challenges you've had engaging with local and state governments? For example, preparing for voter registration databases to the transition to new cryptographic standards. We know that'll be a hot potato when it happens. So what's your thinking on that?

Mr. Hill: Yeah, I mean, you know, ultimately this is going to be about awareness, right? I suspect that if you talk to, you know, secretaries of state or election officials, you know, they are not likely aware that this is a problem that is coming. So that's one of the key objectives of the NSM, is to get departments and agencies – particularly DHS and NIST – to start developing programs to raise awareness among those groups that, you know, have got other things to worry about rather than a – you know, a threat to their cryptography several years in the future, right? They're worried about the immediate, you know, staffing shortages, or whatever they may have.

So, you know, this is going to be an iterative process where, you know, I can imagine that in the next few years you'll have additional guidance coming to the U.S. government about how to engage with these groups that really need that not just awareness but technical support, potentially financial support. Because, you know, these organizations aren't – you know, and likely should not be – experts in this stuff. And they're going to need guidance and some handholding to make sure that they're doing the right things when they need to.

Dr. Lewis: So DHS will be the focal point, then, for engaging with state and local, or?

Mr. Hill: And NIST.

Dr. Lewis: And NIST, OK. Has there been any engagement?

Mr. Hill: There has.

Dr. Lewis: How is it going? (Laughter.)

Mr. Hill: You can ask them. But I – as I understand it and what I hear, it's going quite well. You know, NIST has at the National Cyber Center of Excellence stood up a project that we're hoping to formalize on post-quantum cryptography and thinking through what kinds of products you can develop to automate some of this stuff so it's a little less cumbersome and a little less onerous for IT managers to swap out their crypto, and how to run tests, and all of these things that they're going to need to do.

So, you know, I think at this stage it's really about getting the cryptography right and then figuring out prioritization for the implementation, right, because all across the – you know, the internet ecosystem, there are places that are going to need to be addressed – there are systems that need to be tackled first before we deal with sort of the second-order risks that, you know, can potentially – just have less sensitive information, less time-sensitive information that you can – that need to be updated. But there are more critical systems that we need to pay attention to first.

Dr. Lewis: That's one of the things that's come up a couple times, is that it's probably safe to assume that people are recording and storing encrypted communications. But if it's 10 years before they can read them, a lot of that will be overtaken by events. So the bright side of a long rollout is maybe that helps us manage the risk if we start moving now.

Mr. Hill: Yeah, and you need – you need to think about the time sensitivity of your data, right? If the window where it's, you know, still applicable to either your business or your government agency, you know, if it's a five-year timeframe you can feel pretty confident that if it's collected today you'll be OK. But if, you know, the information is going to still be sensitive and, you know, secretive in 20 years, then you need to start thinking about how do I identify and prioritize securing that data now or as soon as possible, before other less critical information.

Dr. Lewis: Where does quantum fit into infrastructure protection? Because just getting people to use regular, good old cryptography would be a step in the right direction. What's the challenge for quantum there?

Mr. Hill: Yeah, just, you know legacy systems are inherently challenging to update. Some systems, you know, the company that you initially – you know, your vendor that you procured from is out of business and you can't even get an update if you want it. So, you know, the lifecycles of critical infrastructure in particular are long. So, you know, those are going to be key challenges for the next five, 10, 20 years for the U.S. government and for states as well, just to make sure that, you know, those old cryptographic standards that are no longer secure are dropped and safer cryptographic standards are implemented.

You know, it's going to be different for every sector. But clearly, given what we've seen for IT modernization in those sectors – you know, water, energy, transportation – you know, those things are going to take time.

Dr. Lewis: What's the role for Congress in all this? I mean, Congress kind of started it. What do they need to do now?

Dr. Tahan: Well, Congress can always help, right? I mean, Congress has played a critical role in the National Quantum Initiative with the National Quantum Initiative Act. Just recently, in December, they gave us some more work to do, good work. They legislated our Economic and Security Implications of Quantum Subcommittee, which – whose goal – its charter, really, is to cross-brief the agencies so that they're aware of the risks, but also do research and security assessments, export-control assessments. You know, so that's congressionally mandated now, which actually is helpful because it makes it

a much more serious thing for us, very much motivates us to solve it – help solve these problems.

There's, as you can imagine, many different viewpoints across the country. They all talk to Congress – (laughs) – you know, about what they want. So I think, you know, taking a balanced approach to, you know, how can we help industry, how can we help the whole country – you know, at the end of the day, how can we ensure this technology benefits American people, right? So, one, it creates opportunities for great jobs. And, two, as this technology becomes useful, just like AI, how does it, you know, broadly help the country and not just, you know, a few people? You know, those are the things that I hope Congress, you know, will be focusing on.

Dr. Lewis: How much money are we talking about here? Do you need more from Congress? Is the budget fine? Everyone always says they need more, but in a realistic sense how much more?

Dr. Tahan: Well, there's two parts of this. You know, the NQI, you can – you can look up our budgets online. We're spending in R&D, you know, at least 800, 900 million (dollars) a year for all of quantum information science and technology.

The cybersecurity stuff is a little bit more complicated, probably, to complicate – to calculate. But, like, the number-two thing the NSM asked for is this vulnerability analysis. So how many of the systems across the federal agencies are vulnerable and need to be upgraded? And start working with the Office of Management and Budget to do an accounting of that. It has to start there. We can't give you a number right now. So once you know that, you get a sense of how do you equitably do this over the decade in the government and hopefully without the – outside the government as well.

Mr. Hill: Yeah. Just echoing what Charlie said, you know, OMB has got a lot of work ahead of it to try to figure out how much this is actually going to cost, because I think everyone agrees that it's going to be significant. And exactly how much that's going to be we're not going to know for some time, but the NSM lays the groundwork for figuring that out.

You know, I'll say that as much as Congress can fund these basic scientific R&D projects, you know, the better, right? That money goes a long way. You give, you know, a Ph.D. student a small grant, you know, that can pay dividends for years to come. So it may not be as much money as we think it needs to be, but you know, a small amount of money can go a long way and a lot of money can go even farther.

Dr. Lewis: So, last question, from the audience. What does the government need from the private sector to ensure the success of moving U.S. IT systems to post-

quantum cryptography? And I might broaden that a little bit. It's a good question. But also, what does – what do we need from the private sector in this space? So two questions, really: What do we need in general? What do we need for the move to quantum cryptography?

Mr. Hill: Yeah. I'll say perseverance. You know, it's going to be, like I said, a laborious task. It's not going to be fun. It's going to be time-consuming and at times tedious. I think just a commitment from companies to put the resources that they need into this. I think for the big companies, a commitment to help their customers make any kind of migration that they need to make. And to make it easy, right? As much as companies can make these migrations for their end users automatic and seamless where you don't even know that the upgrade has occurred. You know, that will make life a lot easier for a lot of organizations and really reduce the threat overall.

Dr. Tahan: Yeah. I think there's a lot of opportunity here for ambitious companies. For example, the government's going to need help – (laughs) – in understanding, you know, across the wide number of agencies all of the different systems, you know, what do they need to do in terms of to upgrade. But also, if you want to take an accounting every year of how are you doing, you really need automated systems. You know, you don't want somebody with a spreadsheet doing that. (Laughs.) That's not – that's not efficient. So I think there's a lot of opportunity for innovative companies to provide new software tools to make this happen.

And again, it comes to crypto agility. Like, how do we ensure that this dramatic of a change doesn't happen every 10 years but we do it in such a way that it's just sort of automatic as we keep going? Because there's always going to be a new thing, right? People are smart. No – (laughs) – no cryptographic system is perfect. We need to be able to upgrade quickly.

Dr. Lewis: So when should people who want to become entrepreneurs start looking, then, at these opportunities you're talking about?

Dr. Tahan: Oh, the ones I was thinking about are now – you know, yesterday. It's always a good time to think about what problems you can solve, right?

Dr. Lewis: Jonah, anything?

Mr. Hill: Yeah, now, you know. On the cryptographic fragility point, you know, you don't need to have the new standards to start making the internal changes to have a more agile cryptographic environment in your enterprise, right? That process itself is going to take time, even before the standards are released, so start running tests now, start building systems now, so that you're ready to hit the ground running when NIST finally has its standard standardized and widely available.

Dr. Lewis: Any final thoughts? We covered a lot of ground.

Mr. Hill: I'll just say, you know, this has been a really – just, in full transparency, this is an area that I came into very late. You know, I hadn't – you know, I had heard about quantum computers, I had heard about quantum information science but hadn't worked on it much just in my previous role, but just to sort of have my eyes open to this field and people – you know, to get educated from people like Charlie and other experts across the U.S. government and industry, it's a really exciting area of science and tech that has – you know, really could revolutionize fields in ways that, you know, I certainly hadn't realized until I dug into this stuff and was working on these presidential directives. But it's – if I were, you know, in college these days or, you know, had the opportunity to pick a new field, this is something where there are tremendous opportunities both for innovation but also for security, for national security and cybersecurity, so recommend that this – you know, folks who are looking for new areas to work, you know, for young people who are looking for future careers, like, this is an amazing area that's going to be with us for a long time.

Dr. Tahan: I was going to say exactly the same thing. There are great careers in quantum information science now. We need you now, number one. Number two, you don't need quantum technology to protect your computer systems so we are actively running, you know, deployments, you know, develop and deploy for classical quantum-resistant cryptography, so don't take the newness of quantum to mean that you shouldn't start thinking about how to protect your systems. We don't need quantum to do that. So those two key points.

Dr. Lewis: Great. Well, we certainly covered a lot of ground. Congratulations on getting the two documents out. That can always be a struggle, actually pretty quick in terms of how these things go. But Jonah, Charlie, thank you very much for talking to us today.

And as usual, the recordings here will be available on YouTube and all of our other websites. If you type "quantum CSIS" in, you'll get it. We won't be able to take questions anymore but if you do want to view it or view it later for the recorded version, thank you very much for attending today.