HOMELAND SECURITY EXPERTS GROUP (HSEG)

2022 HOMELAND SECURITY ENTERPRISE FORUM

PLENARY SESSION 8:

QUANTUM COMPUTING: HOMELAND AND NATIONAL SECURITY RAMIFICATIONS

Salamander Resort & Spa

Middleburg, Virginia

Wednesday, October 26, 2022

Plenary Session 8 - Quantum Computing: Homeland and National Security Ramifications

 MR. EVANINA: So welcome. Humor start today. Well, good morning, everybody. And again, after the clear presentation, we're excited to get into the conversation of Quantum. And I'm going to tee it up just a little bit for this esteemed panel here with Yosry, Zak, and Matt that are really experts in this space. From my perspective, well, the last things I did in my job, gentleman was briefed to senate on the state of counterintelligence in the United States. Part of that process is to rent -- rack and stack where we are from a threat perspective. It all came down to as it does with China.

 What about China? Well, Quantum is number one, right? So what about Quantum? We talked to the Senate about the numbers, the dollar value investment, you know, open-source. So I think its 11 billion, they've committed to this space, more than not open-source. But -- and the intelligence services of China said, "He who breaks encryption, wins." Right? So it's a big spy issue. That was the premise of the entire brief to the Senate. I'll ask you and I'll –

 Zak, I'll start with you. First, tell us a little bit what you do in your job? And then tell us what is Quantum? Because it's great to talk about how important it is. What is it?

 MR. KELLY: Right, exactly. Thanks. So, I'm Zachary Kelly, I'm with Amazon Web Services. I'm an enterprise strategist where I help our federal customers in the civilian area, think about large-scale long-term transformation. And in those conversations, National Security, Homeland Security are absolutely fundamental. And Quantum is increasingly come up -- coming up. That's why we're here today to talk about it.

 So, when you think about what is Quantum, let's start with the abacus. I'm not going to talk for 3 hours, by the way, as much as I would love to. Imagine a thousand years ago, you're a Silk Road trader, and you're using your abacus, which by the way is a computer. An abacus calculates its store state, it has memory, and it uses algorithms when you calculate with it. It is a mechanical computer. That's an abacus.

 Now suppose the time traveler shows up and hands you a laptop, what do you think of that? Can you even understand it? It's a bit shocking, isn't it? And so, we're going to get there. What's happened is we've gone from a mechanical age where we build things mechanically, to an electrical age, electromagnetism, where we build things with electromagnetism. Modern computers are based on transistors and the state of on and off with bits, right? And that's an electromagnetic phenomena.

 Quantum computing takes us into the realm of quantum science. It's a different kind of science. Just like the person using the abacus, that's us today, can't really understand the laptop, us today are in the early stages of understanding, applying quantum science to ordinary problems. So that's why it's tough to understand.

 So what actually is quantum computing? What I've observed over and over and probably many of you have, is if you go to Google and you look up counting -- quantum computing, you see a lot of big words. You know, you see superposition and entanglement and you know, lots of science and this sort of thing. But do you ever walk away understanding what it actually is? You sort of walk away with, "Oh, it's a big, fast computer."

 Here's what it actually is. You have maybe heard the phrase Qubit. A qubit is the smallest unit of processing in a quantum computer. Right? It does processing and it holds state just like a bit in regular computing -- electromagnetic computing. But what actually is that qubit? Get ready for this. It's amazing. It's incredible. That qubit is an atomic particle or a subatomic particle. It is actually an electron, a proton, a neutron, a quark. That's what it actually is. And a quantum computer isolates or contains these atomic particles and provide state to them with various new kinds of algorithms. And then the properties of quantum mechanics cause those algorithms to be solved. Okay? That's what it is.

 Now, why does it have these magical properties of being able to solve massive complex problems? Because of the properties of quantum mechanics, this big word superposition. All it means is, instead of binary on-off, when you apply an algorithm to that qubit, it can actually have literally an infinite quantity of states, all represented as probabilities within the life of that atomic thing. Okay? And so, when you have a bunch of these together with the superposition, they enter into quantum entanglement.

 So all those possible states with this qubit and all the possible states with this qubit, they become entangled. They actually can touch each other. Right? And so, how do you get a result out of that mess? It sounds like all you're getting is in an infinite amount of states, that's not helpful. What happens mathematically and in physical reality is when that thing is observed a certain way. And this is just normal quantum mechanics, right? Which is weird to us, because we don't think about it and teach it. It's not every day yet. But in 100 years, it'll be every day.

 And so, when we observe that entangled state, the phrase we use it collapses into a single solution. So all of the possible solutions exist in those two qubits entangled until you observe it in a certain way. And then it collapses to one solution. That is a quantum computer. So, you can have many, many variables and extremely complex algorithms. And they're easily solved by this mechanism. Why don't we have it today massively? I'm about to zip it. You know, why isn't it just overwhelming us today? Because there's still some fundamental science to be done.

 A number of companies are building quantum computers with several -- you know lots of qubits in them. And they're doing quantum algorithms and they're running them. But there's a problem. There are two problems that we have to resolve. Right now, today, we can add up pretty much all the qubits that we want. But there are two problems that have to do with quantum science. One is noise. At the quantum level, there is noise. Think of static on the radio, static on the television, that's present. And the more of these qubits you add, the more that noise adds up, and it wrecks your algorithm, and it makes it inaccurate. We have to solve that. That we can likely solve algorithmically. But there's a lot of science going on there.

 The second problem, another big word decoherence. All that means is things fall apart. Coherence, things are together. Decoherence, they fall apart. Think about it, if a qubit is an atomic -- you know it's an atomic particle. Well, how are you containing it? With materials made of atoms, right? So, it's like pouring water into water. If you -- you know, you're containing an atom with atoms. And so, all of this can interact and come apart. So we have to deal with that.

 And there are various scientific ways to deal with that we're experimenting with make it really cold, strong magnetic fields, lasers, material science, attempts to do it algorithmically. That's what's slowing us down. We've got to figure out the noise and we got to figure out the decoherence. When those problems are solved, this will explode. And that's why the timing of all this is so uncertain. So, Quantum is now, but not yet. We've got some now, but the big stuff is coming. Thanks for enduring that.

 MR. EVANINA: So Zak, you validated my concern that I have absolutely no idea what you're talking about. So we can stipulate the facts that I have no idea what you just said, which is why this is so important. Seriously, because quantum is happening, whether we want it to or not, so we're going to -- we're going to take you just said from a scientific PhD level, that I understand, and we're going to transition to Matt.

 Matt, tell us a little bit about what Zak just said, and how this manifests itself in applications in everyday life, and what we can see as an audience in quantum and where it's being applied?

 MR. HAYDEN: So, the easy answer is that in the early 80s, there was someone, akin to Zak's skill set, that communicated to the intelligence community that this was real. And so, long before we had a critical and emerging technologies list, we had a focus on the advantages that would come to anyone that harness this ability. At the same time, the risk to any of our systems, should someone turn this advantage on us?

 And so, there was a national security policy that started to build in the -- let's start seeding money here, there, and everywhere, to make sure we were taking advantage of any necessary plus ups to keep the United States in this conversation. We had a strong urge to start adding it to things, like 5G, counter-UAS, and things like that, and it got a little diluted candidly. Right now, we have applications that are functional in the private sector. We have -- so when we say quantum is real, there are companies that are demonstrating results from quantum computing.

 The applications from a government perspective are very diverse. They are everything from secure communications, secure networking. The obvious answer that we'll touch on in a little bit of cryptography, I mean, the challenge and the risk to undoing one's passwords. But that also doesn't touch the tip of it, because we're really talking about advanced pattern recognition.

 So if you've ever been in one of those labs within the Department of Energy and they're doing an advanced simulation, that on a supercomputer takes a week to render, imagine it takes 5 minutes. That's the way our enterprise is looking at this. Okay? So if I could simulate something, very advanced, that takes astronomical dollars and time, how do I get that in my hands before my adversary does? It's almost as the movies would have you perceive, a time machine because you're getting an answer before you should. And that's the way that the advantages of quantum mechanics have brought a strong risk as well as a strong operational need to the government focus.

 MR. EVANINA: So Matt that puts a little bit more perspective. And I think we're going down the linear compendium of big science, from Zak to application. And Yosry over to you, in terms of this work, who's doing it? Like where is this work being done? Is it in the Government, Department of Defense, Academic Institutions, MITRE; who is doing this? What they're talking about?

 MR. BARSOUM: Thank you. I'm Yosry Barsoum, Vice President of MITRE. I lead to FFRDCs that we operate, the system engineering FFRDC for DHS, and the National Cybersecurity FFRDC for NIST. So, let me just add a little bit to what Zak said. You know, actually, quantum physics was discovered 100 years ago. So, it's not a new thing. It's as people as they started observing subatomic behaviors. The physics of classical physics, like if you throw a ball, you could actually predict where that ball is going to land, what the velocity is, and so on. They applied that to subatomic particles and discovered that the behavior is vastly different. And that's why they -- so it's really the observation of electrons and those subatomic particles that give rise to this new quantum physics, which is different.

 Now, you know, as we talk about quantum, there are really three distinct areas that we should address, because your question, who's doing what, really falls into those three areas. There's computing that everybody knows, breaks encryptions and so on. But there's also communications and they're sensing. They all have different maturity levels at this point. I know, you know, everybody predominantly knows computing. And everybody's working on computing, industry, government. In fact, there was an audit report from the IC Community dating back in 2004, that predicted that we would have they have -- they had a roadmap. And they predicted that we would have a quantum computer by 2012. Obviously, we're not there. There's lots of challenges, as Zak said, in terms of stability of these qubits and robustness and keeping their state, because they interact with the environment and their environment changes their state.

 So, lots of people are working it, you know, in terms of computing. I wouldn't say anybody is ahead of anybody else. You know, industry is working it, government is working, international governments are working it, it's still long ways ahead. In terms of communications, I would say China 2016, they launched their first satellite and that was publicly known, and it is up there, and they're able to do quantum communications between the ground station and the satellite. And, you know, so they're much more advanced than others in that arena.

 When you talk about sensors, sensors are actually that are products out there that are able to detect, you know, changes in gravity. So for DHS applications, thermal detection for example, atomic clocks for accurate timing. So, there are products that are quantum sensors that exist out there that you could -- you could find.

 MR. EVANINA: So let me follow up with you, Yosry, and the mindset you being an FFRDC and having those two specific inroads to organizations that are driving this critical development. From the thematic perspective of this conference and partnerships, do you see the requisite amount of partnerships from the FFRDCs, the private sector, academics, institutions, and the government to be able to compete in this geopolitical world?

 MR. BARSOUM: Absolutely. I think there is, you know, it would anything, things could always be improved in terms of partnership. I'll give you one example. We're working collaboratively with Sandia and MIT on a Moonshot, so it's a MITRE, Sandia, MIT Team to develop a quantum computer. Now, what varies between all these is the material you use. There is about 10 materials now that are out there that people are using. Google is using something called superconductor material. MITRE, MIT, and Sandia are using something called photons and actually, something else called solid state defects for those ladies out there, Diamond. Diamond actually has a defect. Those defects in diamonds is that we're talking about. It has certain properties that can and we are exploiting to build our quantum computer. So partnerships are happening.

 MR. EVANINA: Good.

 MR. BARSOUM: We have a partnership, as I mentioned, but the material is really a key component. To the Zak's point, why are we not here yet? Every one of these materials have advantages and disadvantages. And there's no panacea in terms of one material that is able to physically realize these qubits in a realizable way.

 MR. EVANINA: So to transition Zak and Matt, I'm going to go both you're here. So I spent a lot of time in New York in the financial services sector, healthcare sector. Why are they so intent on investing in quantum, both at the banking institutions and hospitals and some retail organizations? And Matt, I'll start with you. Okay.

 MR. HAYDEN: So, when we first started talking about encryption, it was based on financial transactions, because they wanted to have a secure way to know who was making this transaction and what was the quantity being transferred. If you tell the financial industry that there's something that's going to rattle that, they're going to fix it the fastest, because they know where their challenges lie in that world. So they've invested in it. But it's not just a protectionary measure. They're looking at it as advanced analytics.

 You can get insight into where a particular crop is going to grow, you can do all of the things that we hear about huge hedge funds investing in to try and get predictive models on where the state of our economy is going to be, where these next spikes are going to be; all of that information can be simulated in a way that just can't be done now. So, from the financial sector, there's that advanced insight, there's that protection needed. And they see the use cases, which is the important throwback to the national security window of what we have to do next, is the financial services has taken a look at this technology and said, "Here's how we can use it and here's where our risks are."

 The federal government has done the same thing. But when we start looking at where our risks, we got hung up really quickly on encryption. We said, "We have archives and archives of materials. Do we even know what encryption is on that now?" And moving past the encryption conversation, there's use cases that we need to build out, whether it is, as we say to some of the things around sensors and communication technologies. But that's the effort. It's stopping and taking a look at where those use cases are in our mission focused world, as well as the broader economy implications.

 MR. EVANINA: So Zak, same issue, same thematics, but add in the fact that, as we hear in Homeland Security, where the difficulty we have in tying things together and having a holistic look at protecting our nation. Same issue from application, why it's important for financial services sector. But also the lack of talent in cyber, how are we expected to be successful in quantum if we can handle the cyber demand right now?

 MR. KELLY: Okay. So there's good news and bad news. And the good news is the near-term threat from quantum is manageable. The near-term threat is that certain types of encryption algorithms may be breakable by quantum computers in relatively few years. Some people think maybe as soon as 3 to 5 years, some people think maybe 10 years. But I think that 10 years is a pretty safe bet that certain types of algorithms in use today may be broken, which means certain types of data may be at risk of being decrypted.

 The good news that that's really what's coming quickly that could affect our homeland and our security. And so, it's good news because we've already been through this before. Cyber professionals, IT professionals have been upgrading encryption algorithm standards for years. This is nothing new. We have to continuously upgrade those standards. That's why we have FIPS. That's why we have NIST. And that's why we have federal guidance that tells us what to do, when to do it, how to do it.

 And so, moving toward quantum safe algorithms for this first wave of susceptible encryption, it's a pretty straightforward exercise actually. And NIST, as you may be aware and we'll probably get into this question, has done quite a lot of work to standardize what types of algorithms you should move to. So, future threats will become much, much more aggressive than this, but they're pretty far out. We've got some real fundamental work to do. Fundamental science before some of the very powerful brute force attacks can happen and the modeling attacks can happen. That's pretty far out still.

 MR. EVANINA: So with that framework, Matt, still concerned about human resources here, right? So from a government perspective, we are still in a quagmire of understanding where supply chain sits in the government, who owns it, who's in charge of it? Take us to quantum now, right? So CISA insights out to you know, in the post crypto world, we're not even a pre crypto world yet, but what's, you know, an admonition. In your vision, 4, 5 years from now, who owns the programmatic efforts of crypto and in quantum bigger picture in the U.S. Government?

 MR. HAYDEN: So the intelligence community is going to take the lead on a majority of this. So when CISA comes up, they're going to be that engagement arm with industry and critical infrastructure, as well as the DotGov civilian space. So, there's a partnership there as well as learning what private sector has to offer, because as what's just said, the NIST operation is a very transparent and public campaign to solve some of these algorithmic challenges.

 The good news is, from a human resources perspective, we're actually going to get to leverage tools, we didn't have a long time ago. So there's going to be the opportunity to leverage things, like Cloud resources. So, when we look at quantum algorithms and big compute -- or quantum machines, this is something that Cloud can lean in and start to give us some of those tools and some of those protection efforts quicker. So, we're not talking about training every human out there to try and learn a new algorithm. We're training everyone that currently maintains algorithm, how to swap those algorithms out, identifying catalog where they are, and to work in more of a mechanics pace, as opposed to someone that's more of a data scientist. That doesn't mean we don't need more people. It just means we're finding ways to support what we have with what we need to do.

 MR. EVANINA: Good answer. Yosry, on that one, right, so same linear path. So taken what Matt just said and proceeded with Zak, are we looking to hire cyber professionals, data scientists, PhDs in physics or a combination thereof, to facilitate the progress we're making in quantum?

 MR. BARSOUM: I would say, it's more of quantum engineers. People who understand quantum, but could apply it, you know, to both cryptography as well as some of the new algorithms that are going to be using, you know, quantum computing, quantum sensing, and so on. So, I think it's a new breed of, you know, what I call quantum engineers, that would be required.

 Just like in the early days, we had spectrum as it became a war fighting domain. We had spectrum specialists and so on. I think we're going to have a -- it's not a physicist. It's not a, you know, an expert in quantum. It's not a cyber. It's sort of a combination of things. And I would sort of bucket that as quantum engineers.

 MR. EVANINA: So, with that being said, from a minor perspective, let's put the government aside for a second, let's put the financial services sector aside, where does buyer find those people? Do they exist currently?

 MR. BARSOUM: Well, I would say they exist in very small population. The whole community is a very small population. You know, we have a handful of world renowned, you know, quantum physicists, but they're very, very small. I think that, you know, just like cybersecurity became a domain that is taught in universities and colleges. I think we're going to have to have some training that really is focused on a quantum area. And hands on, you know, education on the job.

 But do they exist? I don't think they currently exist. I think what exists right now is really physicists who understand the physics of it, that understands the materials, that understand some of the implementations. But we need to go beyond that, you know, into this engineering realm that you don't necessarily need to have this in depth, you know, physics background. But enough of an understanding to be able to utilize the capability and ensure that the capability, you know, is maintained and upgraded as time goes on.

 MR. HAYDEN: To add to that for just a moment, most of the companies doing research and development in quantum computing today also have incubators for doing exactly what Yosry is saying. They also have a group that's teaching, that's putting out educational materials that's giving simulators, so people can use it. And so, it's in the infancy, but we're beginning to build the capability that Yosry just mentioned.

 MR. KELLY: In fact, if I could follow up. Our quantum group is actually co-located at Princeton University. And they're starting in that education track as well, just as an example.

 MR. EVANINA: So with this excitement, even though I don't understand it, I'm excited about to hear the progresses and amazing thing in a super modern developed world. But I come from a really dark and dreary depressing world, right? So with this progress are we collectively, I'll ask all three of you, are we collectively in all of your world as we're working in partnership, are we building this new platform with the requisite protections in place, knowing that we can handle the cyber protections now, critical infrastructure and so forth; are we doing the right things prominently to protect us and the industries as we succeed in quantum? And if not, whose responsibility is that? I'm going to start with you.

 MR. HAYDEN: So I started with way before there was a critical and emerging technologies list, that list does exist today. That includes a whole of government strategy to look at all the processes related, the material science, the investment materials, the technology. And the way we look at, the way we look at semiconductors right now. So that's the same lens that the government is using from a protection standpoint. If there is a jump in technology, how are we going to lean in to assure the security, safety, and way of life of the U.S. citizens? And so, that perspective carries and there aren't specifics other than partnership at the moment.

 There isn't a you know, 4-nanometer example where we want to put restrictions on export or anything like that. There is a pure science model right now. But as it evolves, there is that knowledge and notion that for things that may fall into the wrong hands, we're making sure we're aware of those types of things. But it's not to a protection stance yet. So that's -- the good news is the operational focus of a lot of these technologies haven't reached that operational cadence to where it's a challenge that needs protection as much as it needs evolution.

 MR. EVANINA: So with that Zak, do we now become concerned with not only hackers and debasement and criminal hackers in Europe, nation state threat actors having the capability to do what they do now on steroids. Is that a concern?

 MR. KELLY: We absolutely do. That's why this is becoming a conversation in the security community. It's time to start thinking about it. It is not time to be alarmed. It's not time to think we're going to be cracked next week, you know, by an adversary with a quantum computer. However, those near-term algorithms, encryption algorithms, there's something to think about and for enterprises to begin planning, upgrading to the new algorithms. Now is the time to start planning that, take a look at what NIST is doing.

 In terms of the longer term picture there are enormous potential threats. And they're really in two categories. One, is the threat of malicious actors who are using the features of quantum computers for attacks or not just attacks, but to model our responses, because our responses to attacks could be modeled so precisely that you have a little bit of back and forth gamesmanship, and we could be halted in our responses.

 The second piece is simply the cultural implications of this kind of technology. Think about it a lot like AI, strong, independent decision-making artificial intelligence. So back to the regulatory question, how do you control it? Ultimately, I believe government regulation will come into play and must come into play around some of the new technologies like strong AI and quantum computing.

 MR. EVANINA: Yosry, with that same framework, we used to always say and still say in the cybersecurity world, behind every massive breach, there's a human being. Will this change now? Will this allow those breaches to be non-human generated?

 MR. BARSOUM: It could be -- it could be. I would just add, you know, from a threat perspective, you know, to your original question about, are the controls in place? There's this dichotomy. This still exists largely in academia. So, academia want to publish. They don't want to control information. So, you know, there's this struggle of, you know, I want to publish to become known in the field versus I want to control the information, because adversaries may have access to it. You know, from a threat perspective, I'll just add to what Zak said, it's really, you know, it's been known, and you probably know better than most adversaries have been collecting a lot of encrypted data from us and everybody else in the world. They haven't been able to break it to sort of glean any information. But once they have a quantum computer, they're able to break it in from the past, to learn about strategies, to learn about capabilities, and so on, and so forth.

 So, I think what, you know, when we talk about post-quantum cryptography, it's really important not to wait until we have a quantum computer to counter that effect, but really develop it now, so that we don't give them the opportunity -- don't give the adversaries the opportunity to be able to continue to collect and then crack the code when a quantum computer is available.

 To your question, I certainly believe that yeah, the answer is yes. Is there going to be a human? I think a human will still be there. Will it make the job easier to, you know, be able to crack into networks and penetrate that? I believe that would be the premise.

 MR. EVANINA: I have one more question before we open that up to the audience. So, 10 years from now -- 8 years from now, when, what's his name over there, he's having our 10th anniversary at the conference, right? And what we're -- Robert, yes. We're here for celebrating the 10th year of this forum. Give me one area where the audience could expect just tangible real life improvement with quantum in 10 years.

 MR. HAYDEN: That would have been a theoretical 10-year mark, that's a tough one. We do have the ability to think differently with large sets of data. So pattern recognition will become more efficient, even before we have quantum computing really at our doorstep. So, there's opportunity right now that we can use to look at things with kind of a quantum enhancement, if you will. But we take our current view and try to get to that pattern recognition set to find that needle in the haystack faster or to find what we're not even looking for to train an AI to find it faster. So, we're looking to see those two become more integrated.

 So, my statement would be the technology jump in 10 years is that we're using quantum techniques to empower the training data and algorithmic integrity of AI. And it's become a leap in itself.

 MR. EVANINA: Great. Zak, what do you think?

 MR. KELLY: Yeah. Something very relevant to Homeland Security is bringing quantum computing to drone optimization to protect the country. Quantum computing can optimize distribution of monitoring-type of drones in key areas where they're highly needed. And then quantum computing can optimize understanding the data that that -- those drones are collecting in order to detect whether there's a threat combined with AI, as Matt is saying. I think we will see on approximately a 10-year timeline, really dramatically enhanced drone management with quantum computing?

 MR. EVANINA: Yosry, your thought?

 MR. BARSOUM: Yeah. You know, it's hard to predict what happens in 10 years. But -- (cross talk)

 MR. EVANINA: I'll have to, that's my question.

 MR. BARSOUM: I would say what's really promising are quantum sensors. You know, you think about what does a quantum sensor provide you? As a rule of thumb 10 times what a traditional sensor provides you. So, you know, you could imagine putting a quantum sensor on a UAS at the border. And you're able to maintain that UAS in the air for longer periods of time because it doesn't require -- the sensors don't require a lot of power, a lot of size, and so on. So, I think the world of sensors -- quantum sensors are really going to be making a splash in the next few years.

 MR. EVANINA: Good. All right. Out to the audience, if anybody's brave enough to actually ask a question. Yes, sir.

 UNIDENTIFIED SPEAKER: That was just brilliant. Just fascinating. Thank you very, very much. Absolutely fascinating. So important in so many areas that you've cited. My question is this, what are the first mover advantages? I come from the private sector, first mover advantages. What do we lose if we don't get there first? And what do we gain, if we do? What keeps -- if someone gets there first, what keeps others from simply knocking it off? So within days, weeks, months or a few years everybody's got it versus is your high wall?

 MR. EVANINA: I'm just putting in that, is everybody going to have it or is it just really us in China? And what is that first advantage? Anybody in the panel?

 MR. KELLY: Well, I'll say, initially, it will be in just a few parts of the world, in major Western countries, China, certainly. But eventually, this will become a ubiquitous technology, like all computing technology. There is an enormous first mover advantage because of some of the problems you can solve with quantum computing. Let's just take one example that's relevant for national security and homeland security, material science. Quantum algorithms will allow us to design new materials, that we're not even thinking of yet, and we can't design today. So, we may have armor that can withstand a missile and it weighs next to nothing.

 These are things that can potentially come from quantum science. There are many other areas in biochemistry, genetic research, because we can solve problems at a scale that we can't even imagine today.

 MR. BARSOUM: I'll just add a little bit to that. There's lots of investment that's going into these startups. You know, 5 years ago were not a lot of startups in this area. There are hundreds of startups now. You know, I'll just point to one, "SandboxAQ," nothing, you know, special without investing in that, but that just received, a startup that received a billion dollars from Eric Schmidt, who ran Google before. That's an unheard of for a starter to receive that amount of money. So, there is a lot of the first mover advantage, as Zak was saying, is able to design drugs, is able to design vaccines. The power is enormous. And a lot of the investors are seeing that potential. And they're putting their money into it. So, there is a first mover advantage.

 MR. KELLY: And then the added challenges, it's not just a single use. We're not talking about a national security focus. It's a dual use. So when we're talking about biometrics and things of algorithmic back end, like block chain and things like that; everything that has like a standard that we look at from a security perspective, could have a different wrinkle once these technologies are there. Everything from batteries all the way through to anything that uses a signature is a unique application that can be found. But there could also be incentives in the private sector that are kind of that bank shot for national security.

 MR. EVANINA: Okay. Yes, sir.

 UNIDENTIFIED SPEAKER: Yes, sir. As the resident English literature major, it makes build look really good in this area. My question for you all is what is your greatest concern about the development of the quantum mechanics now?

MR. KELLY: Well, sir, I am an English major, so I applaud you.

 UNIDENTIFIED SPEAKER: We're too.

 MR. KELLY: That's right. My greatest concern really comes back to human nature that governments struggle to provide freedom and appropriate governance. That's what our country is about. That's what we want. These technologies that are emerging, not just quantum, but AI, and some biochemical technologies, genetic technologies; the world will be a different place pretty soon, probably in many of our lifetimes. It will be an unrecognizable world. What are people going to do with this? That's my biggest concern. When you can solve problems that today we can't even imagine, are we morally, ethically, psychologically, emotionally, able to handle that?

 MR. BARSOUM: I would say there are two areas national security and economic security. Those are the two areas where whoever has this capability create that dominance in those two areas.

 MR. EVANINA: Matt, last stop.

 MR. HAYDEN: One of the challenges that was mentioned was past encryption standards. And – and when we have adversaries grab whole sets of data that they technically can't use, what are the conversations going to be when everyone's secrets are on the street? And so, when we start talking about a company that has been extorted through ransomware and they're using their data to put on a cloud to say to demonstrate, "We have your data and we're willing to put it out there if you don't pay us?"

 Now, imagine that a country is held hostage to that same technique. We have all of your national security secrets, how much are you willing to pay to keep those quiet? And so that's the perspective that is a really keep you up at night kind of answer.

 MR. EVANINA: So Yosry, Zak, Matt, I want to personally thank you for making my head hurt and for being incredible experts in your field because I think as Americans, we are proud of our historical progress and innovation, and you three are part of that ecosystem. And as an American, I thank you for doing that and I'm humbled to be on the stage with you. And for our audience, let's thank them for their participation. Thank you very much.

 (Applause)

\* \* \* \* \*