Lauren Williams:

Hi everyone. I'm Lauren Williams, Senior Editor for Defense One. Thanks again for tuning into today, the first day of the GovExec Cyber Summit.

From the Colonial Pipeline ransomware attack to Russia's invasion of Ukraine, cyber attacks are on the rise in war and out, and defending against such attacks requires strong partnerships and active collaboration.

To talk more about that, I'm joined by retired Air Force Colonel Jen Sovada, who now serves as President of Public Sector for SandboxAQ.

Jen, thank you so much for being here.

Jen Sovada:

Lauren. I'm excited to be here and looking forward to a really engaging conversation,

Lauren Williams:

So just so we can do a quick intro, tell us a little bit about what's on your plate at Sandbox and where cyber defense really comes in.

Jen Sovada:

Yeah.

So interestingly enough, we are dealing in all sorts of areas of cyber defense at SandboxAQ.

SandboxAQ is actually a company that spun out of Alphabet about 14 months ago, came out of stealth mode, and we're totally independent now. But we focus on quantum technology that is here today.

And we do three primary things. One is simulate quantum computers using classical hardware to solve very interesting problems like drug discovery.

We are doing quantum sensing, so we're doing quantum navigation, which is related to, what do you do when GPS is denied or spoofed?

And then finally, we are looking at providing the ability to do cryptographic management and encryption management for things like post quantum cryptography. So what happens when quantum is here and you now have traditional algorithms broken and you're no longer able to secure your network?

And so from a cyber perspective, cyber can jam and spoof GPS. So that's one aspect of it.

And then the other one is from post quantum cryptography and making sure that we are protected against quantum attack.

Lauren Williams:

Now quantum, there's definitely some discussion of quantum. It's here, but not really.

Can you make it kind of relevant to what's going on today? I'm specifically thinking of Russia's invasion of Ukraine, and obviously there's a lot of cyber implicated there.

Can you talk about where you're seeing kind of quantum fit in, at least maybe even from the lessons learned standpoint?

Jen Sovada:

Yeah, absolutely.

So there's a couple different things. One is that quantum technology is here today. That's the thing that most people don't know.

Quantum computers are not quite here yet. But what we do know is that when a quantum computer is here that it will be able to crack traditional encryption.

So think of RSA, elliptical curve, Diffie-Hellman, and all of those other types of encryption that we use today to really secure two billion devices globally. Whether it's your handheld phone, whether it's a network, it's your APIs, whatever it may be.

And things like in Ukraine, when the satellites were jammed or they had cyber attacks on their systems; all of those things need to be protected. And some of the ways that we can do that is through post quantum cryptography married up with Zero Trust and enable that whole system of trust within the quantum network space that we have.

And what we have seen, especially in this space related to quantum, is that both Russia and the Chinese have substantial quantum programs.

For example, China has spent over 10 billion dollars on quantum alone. We compare that to the United States; the United States' Government quantum initiative, the National Quantum Initiative, is about 1.4, 1.5 billion dollars. And when you add in venture investment, it's only up to about five and a half billion dollars. So China's spending double what the United States is.

Lauren Williams:

And what does that translate to in terms of effort and developing capabilities? Because like you said, quantum computing is not quite here yet. Is that concerning that the US is being outspent here?

Jen Sovada:

Yes, it is concerning. And for two primary reasons.

One, the Chinese are really focused on two main things. One is the PRC is looking to really develop a quantum computer for one sole purpose, and that is to crack encryption. Whereas the rest of the globe is looking for other uses and ways to enable quantum computing to make the world a better place.

The second thing that China's doing with quantum computing is developing a quantum secure network.

And so when we think about this from the alternative of cyber perspective, they want to secure their entire infrastructure, from their military communications, their research and development communications, and their government communications, as well as some of their businesses, from anyone being able to intercept what they're doing.

So they're building their own ring while many of us are still looking at the traditional types of encryption.

So from that perspective, they could become not only a country that is able to get as much data as they can from cracking encryption, they can also seal off themselves from being able to be attacked themselves.

Lauren Williams:

So I guess to be slightly more, I guess, optimistic, what are some of the projects or initiatives, things that you're watching the US militaries develop that you think would be able to [inaudible 00:05:59] a quantum thread?

Jen Sovada:

Yeah.

So interestingly enough, the US government has a big emphasis on this right now, really since 2018, when the US government started the National Quantum Initiative and then started with different cybersecurity acts.

There was the Zero Trust Cybersecurity Act in 2021 with an executive order. There have been executive orders related to quantum and post quantum cryptography; in particular National Security Memo Eight and National Security Memo 10.

And then in November of 2022, the Office of Management and Budget released a memo that stated that all agencies, federal agencies have to migrate away from quantum vulnerable cryptographic systems to ones that are actually quantum resilient, quantum secure, or post quantum cryptography.

So there's a lot of effort right now across the government to, first, inventory your systems. So you have to inventory all of your encryption; What is out there? What is current? What isn't current? And what needs to be migrated to post quantum cryptography?

And then the second thing is to really develop that strategic plan for how you're going to do it.

The last time the US government migrated their encryption, it took about 20 years. So we know right now that quantum computers could potentially be here in seven to 10 to 15 years, and if we don't start now, our adversaries are storing now to decrypt later. They're taking our data, they're putting it in their own file systems, their own data warehouses, and preparing for the time where they're able to decrypt it instantaneously.

Lauren Williams:

You mentioned it a little bit earlier, but how does this relate to Zero Trust, which is something that the Defense Department, and even outside the Defense Department, there's moving to this architecture, or this framework, this thinking of, "You're already compromised, basically trust no one", making sure everybody has the appropriate access to the network.

Can you talk about how these things are related? Or maybe they're not at all?

Jen Sovada:

Yeah, they're actually very related.

So as you mentioned, Zero Trust is really moving away from the 'trust but verify' that we've had for decades and decades, and moving to a 'never trust and always verify.'

And in the meantime, post quantum cryptography is really looking at, "How do we protect public key encryption from attacks from quantum computers?"

And what happens now is that we can marry the two of them up to create that trust identity that we need to enable trust identity, access and encryption that is all wrapped together, that enables continuous monitoring for not only the individual, but also for the cryptography that you're using, and then enables us to have a foundation of Zero Trust for that post quantum world.

Lauren Williams:

And I feel like you're going to know this better than I do, but is this something that is actively ... ? I mean, is Sandbox speaking with the Pentagon on incorporating this as they move to Zero Trust, or is that something that remains to be seen?

Jen Sovada:

We are talking to the Pentagon and the rest of the government, and we're also talking to traditional Zero Trust providers, to say that, "Hey, Zero Trust is an amazing capability, something that we need to do. Because we know that there's going to be breaches. We need to be able to analyze the behavior. We need to look at whether or not our architectures are designed properly."

But the same thing needs to happen from a post quantum cryptography perspective. And just because you're protected and safe from a Zero Trust perspective does not mean that you're actually secure from a quantum attack.

And so the two actually need to go hand in hand so that you get that total encapsulation of cybersecurity.

Lauren Williams:

And I guess, so I can visualize this, what would a quantum attack look like?

And then also related probably just tangentially, how would this affect the sharing of data? Because I know that's become very important across the department.

Jen Sovada:

Yeah.

So a quantum attack isn't much different from what we see today.

What would happen is that there would be an exfiltration of data off of a network, like it happens in a regular way. And the only difference is is that the device that is looking to try to decrypt or crack that encryption, instead of being a GPU, a graphic processing unit, or a CPU, it's now a QPU, a quantum processing unit. It may be in the cloud or it may be a computer that looks like one of the chandeliers that you see that's a traditional quantum computer.

And what would happen is that there's just faster processing of that type of data. They're able to look at things a little bit differently in how they manipulate and maneuver data.

What happened is, in 1994, there was a gentleman named Peter Shor who was at Bell Labs, and at that point in time, he discovered that regarding traditional encryption, where we just add more numbers, we create factors, the factorization of numbers in the prime, that it didn't matter how many more numbers you added, that a quantum computer could break factorization.

So that's the key behind a quantum computer, is that because of its ability to break factorization, you now have to look at different types and different ways of establishing your cryptography.

Lauren Williams:

And pivoting just a little bit, because we talked about Ukraine and some of the lessons there, but as the US focuses in preparing for a potential conflict with China, we've talked about China outspending the US particularly when it comes to quantum, can you talk a little bit about some of the challenges you see there when it comes to cyber defense and also this quantum?

Jen Sovada:

Yeah, absolutely.

So interestingly enough, and as we know, as we come into a conflict with China, it's probably going to start as a cyber attack or a cyber war.

We don't know if it will be quantum or if it will just be a traditional ... Quantum based meaning they'll have a quantum computer or not. It depends on the timing of when that happens.

But I think one of the things that we can assume is that we're going to be in a very denied environment. And the way that we need to protect ourselves is to try to figure out, "How do we protect ourselves to the edge?", and then create those abilities for us to continue to both communicate as well as navigate, whether it's on the seas with ships, or whether it's in the air.

So for example, when you have all of your devices, they still need to be able to be protected. You don't want to give away your data. So those need to be quantum resistant.

And then from a navigation perspective, we need to look at alternative P&T, alternative precision navigation and timing, in order to make sure that our ships still know where they're going, and that our planes still know where to fly and potentially drop bombs or do other kinetic effects that enable us to persevere in an environment like that.

Lauren Williams:

And what would some of those alternatives be, or to what extent are you guys having those sort of conversations?

Jen Sovada:

Yeah, there are a number of working groups and task forces that are right now active in the Pentagon related to alternative P&T. And they're looking at a variety of different types of solutions. There's visual, for example, using video visual.

There's also a thing what we're building at SandboxAQ, and just recently flew with the Air Force, is quantum navigation using quantum magnetometry. It's where you use the crustal field of the earth that builds a magnetic map, and then you navigate using that magnetic map.

And people always ask, "Well, what happens when the magnetic poles flip and the magnetic field changes?" And what we say is that we don't use the polar magnetic field, we actually use the crustal magnetic field, which is stable, besides minor tweaks, for hundreds of years.

Lauren Williams:

That's absolutely fascinating, and I feel like I need to kind of see this in action, but I am completely enthralled.

So I feel like I have to, because it's the topic du jour now; generative AI, automation, ChatGPT. Where does this fit in with the quantum cyber defense discussion? How are you tracking this?

Jen Sovada:

Yeah. We think it's going to be revolutionary. I mean, it already has been with what we've seen to date.

From a cyber perspective, think about ... I talked about the factorization of numbers and how you get to a prime number. When you combine generative AI that could potentially go through numbers very quickly and you add that to the compute power of a quantum computer, you could have a very powerful capability that could then exponentially, potentially accelerate that encryption cracking.

There's so many other ways that we can use generative AI for good. There's also the ability to look at solutions and other things that could be out there.

Even in the bio-space. We think about when we're creating new drugs and trying to make sure that we're protecting ourselves from people stealing our data. We could potentially look, by using generative AI, and find different proteins and different things that bind more quickly by using generative AI, for example.

Lauren Williams:

And I want to ask, what do you think is missing from the overall cyber defense conversation? Obviously, we've been discussing it's become increasingly important over the last 10, 15 years, but I can't imagine that all the points are being hit and everybody's doing everything perfectly. So from your perspective, what do you think is missing and what do you think needs to be changed?

Jen Sovada:

Oh, yeah.

I think one of the big things that's talked about in some circles and not in others is that cyber's no longer a hardware problem, and we need to stop thinking about ripping and replacing our hardware in order to create better cyber solutions.

In reality, it's about crypto agility and the ability to continually update and modernize your cryptography as new technology comes online. And more often than not, that technology is going to be software based.

And so how do we re-architect our system so we only have to do it once and then enable that cryptographic agility in order to continually be able to thwart new threats as they come along?

Lauren Williams:

I hear you say that and it makes me immediately think of how buying software, implementing software updates has been just a challenge for the Defense Department, even though you definitely hear that rhetorically how it's not just about hardware anymore, it's about software and being able to upgrade, frequently change.

But I think about quantum, and I just wonder if we go from recently having struggle implementing something like Microsoft Office 365, having that, having Teams everywhere ... I mean, that was revolutionary, truly. You know, you add something like Quantum to this, part of me just foresees maybe some difficulty there.

What do you think the department should be doing to make sure that they are adequately prepared across the entire enterprise for this threat?

Jen Sovada:

Yeah, I think that they need to be paying attention to what NIST is doing.

NIST, for example, has a post quantum Cybersecurity Center of Excellence, and they are the ones that are approving the new algorithms and the new standards that are going to be released in 2024 to protect against quantum attack.

And as long as the government is following that, they will understand what needs to be done and be able to prepare and understand that crypto agility is really the way to go.

And also to get people who do cost estimates and others educated on what it means to do software as a service and to do new technology and algorithms so that they don't undercut those cutting edge

technologies and those cutting edge companies that have this technology by lowest bidder, whereas it's really about performance and capability and protection.

Lauren Williams:

And just to wrap up, I want to look to the future a little bit.

What are some of the initiatives, goals, benchmarks that either Sandbox has going on or that you're looking forward to seeing in the next year or so? What should we all be watching out for?

Jen Sovada:

Yeah. From a Sandbox perspective, we're really excited about our Security Suite that we recently launched, which contains both the inventory, a control panel, as well as the initial phases of remediation for post quantum cryptography. And I think that you'll start to see that appear in the government hopefully in the next year.

And I'm also really excited to see globally NIST publish the standards for post quantum cryptography and see the global systems start to adopt ways to protect their systems, whether it's part of their governments or part of the critical infrastructure globally, so that we can protect against adversarial attack that could impact our entire economy, national security, as well as our livelihood.

Lauren Williams:

Jen, thank you so much for being here. It was great speaking with you today.

We've reached the end of our time, but I want to thank you all again for joining us today.

Up next, Tim Rahschulte of the Professional Development Academy continues the conversation on cybersecurity collaboration.

For Defense One, I'm Lauren Williams.