David Forbes:

I was thinking about this. You don't want to follow lunch, right? And you don't want to necessarily go before the happy hour. But following a coffee break isn't a bad way to go, you know? So I think that-

Audience:

We're alive again.

David Forbes:

Yeah, everyone's fired up and full of some good caffeine. I think that that's kind of a good precursor to get into the topic here that I'm going to talk about here this afternoon. Having the opportunity to address a group like this of cyber professionals who are engaged and informed and really enthusiastic about making a difference in this community that we're in kind of sets the stage for me taking a few minutes about talking about our cyber threat landscape as one battle space. So probably you'll find as I go, it kind of takes some different twists and turns and probably instill a little bit of cyber fearmongering back into the discussion here a little bit, which is, I guess we all should have in some way, shape or form in a cyber discussion.

So I want to talk about the cyber threat landscape and explain this whole notion that we are really operating in one connected battle space. And before I do that, I just want to do a little context setting. So I think building on what's being discussed over the last couple of days, we're really at an inflection point in cybersecurity in the United States. The Biden administration recently released the second national cyber strategy as we're all aware of. But we're seeing a couple of very significant and major influences in our future, right? Where do we go from here and what's driving that? For example, we're seeing the exponential increase in connected devices, an unbelievable increase in this space. 13 billion plus connected devices in the world, and that's expected to double in five years, right?

So think about that. There's only about 8 billion people on the planet. So we are moving towards an environment we have twice as many connected devices in the world. And related very closely to that is this convergence of our digital and physical world. Some could say that up until this point with the growing number of IT and OT enterprise devices, there are some pretty clear lanes along the way. But what we're seeing with the reliance on cloud and software as a service and 5G and satellite communications, those lines are really blurred. More and more, year after year, we're seeing that this battle space is a lot more overlapping. It's a lot less clear where the lines are and who governs what space and what drives those decisions. So no boundaries is what we're seeing, right? And this presents a very significant opportunity for our adversaries. Our adversaries see this increasing battle space and they seize it as a growing opportunity to disrupt and deny our most critical assets and platforms.

So kind of going forward here, talking about critical assets and platforms, I'm talking private sector, public sector, Department of Defense, and different agencies, healthcare and so on. I'll refer to many of them along the way. So kind of key point number one here is that when our adversaries look at the United States, they don't see a Department of Defense, they don't see a federal government, they don't see a department of Homeland Security, they don't see a pharmaceutical business. They see one connected battle space with a whole lot of seams and a whole lot of opportunities and a whole lot of vulnerabilities.

So if we're really going to think about this one connected battle space, this type of threat landscape that we're living in now, this requires us to think differently. This requires a holistic view of cybersecurity and a different understanding of that cyber threat landscape. So we've spent decades now building towards this point where we've found ways to create solutions, to create cybersecurity environments for our

critical assets and our infrastructure. But going forward, how we build and how we hunt those threats really needs to change. It needs to change in the innovations that we have and it needs to change in the way that we think. So let me just give you once over the world about what those threats kind of look like. And a lot of this I think connects to the discussions that we've had yesterday and throughout the day today.

Look at ransomware, right? One of the indications of the evolution of cyber trade craft is ransomware, which at one time is moving away from random global blast of ransomware attacks to worm-based ransomware focused, targeted attacks, very sophisticated ways that adversaries can penetrate those seams. Supply chain attacks, right? Look at Log4j. That was interesting, right? Log4j impacted 3 million devices. 3 billion devices were impacted by Log4j. And SolarWinds that has been mentioned many times here over the last couple days. 18,000 customers were impacted by SolarWinds. Zero-days, right? Zero-days for an adversary is a key way to set the stage for more sophisticated attacks. The more complex and the more intent of the zero-day attack, the more destructive that attack could be. So a 2022 Mandiant report tracked 55 zero-days. Okay? That's twice as many as 2021.

Ransomware as a Service, I think it was mentioned here on two panels ago, talking about these attacks as a service. Ransomware as a Service is another way that demonstrate the sophisticated nature of our adversaries. So it's important to understand that this attack surface and the sophistication of these threats is really moving very fast and very quickly. So with that in mind, I want to turn a little bit on this discussion. I want to talk about what the hackers think. We talk about hackers a lot, right? But we tend to talk about hackers in the abstract. But when you think about hackers operating in support of nation states such as Russia and China, you really need to understand the strategies that they're supporting. Step back for a minute, talk a little bit about Russia and China, right?

Russia has really kind of made its reputation with kind of blunt focused ransomware attacks against US critical infrastructure. The momentum of these attacks really started to ramp up after the 2015 Ukrainian power grid attack. We have watched Ukraine unfold. What we're seeing with Ukraine and Russia's cyber involvement is kind of a view of the first hybrid war. And even though that the success has not been overwhelming, it's very clear that Russia has made cyber attacks as demonstrated by the ViaSat terminals being disabled before they started their invasion. That is a key part of how they plan to attack and conduct operations going forward.

China? Motivated by industrial espionage. IP theft is a key part of China's strategy. This theft of United States intellectual property has been seen in the defense industrial base, the pharmaceutical industry, and even in the commercial aviation, auto, and so on. Think about it, the Comac C919 aircraft developed by China is very similar and a direct competitor to the Airbus A320 and the Boeing 737. So these are the kinds of things that we're seeing from two of these most well-known adversaries. So we spend a lot of time thinking about risks and vulnerabilities, but what we really ought to be doing in parallel is thinking about how do we look at things through the eyes of our adversary? Okay, so what I want to do now that we talked a bit about the nation states, how are those hackers doing business in support of those nation state strategies?

So let's think about the supply chain. When hackers get the task to conduct a cybersecurity and a cyber offensive strategy against the United States for example, they're looking at life cycles. They're looking at life cycles of platform and manufacturing and infrastructure and auto and aviation. And those life cycles consist of design, development, manufacturing, operations and maintenance. All these different phases, right? And in some way, shape or form, all of us go back to our organizations and we deal with some sort of lifecycle on the private or public sector. But there are six things that hackers do in each of these different phases of the lifecycle. So let's talk about the design, development and manufacturing phase of

a given system or platform. It can be a weapon system, it can be a space system, it can be an automotive system.

So the first is the traditional hacker methodology, which is to target IT systems. We know this, it's kind of been around since we started trying to tackle this cyber problem. This is very common in the defense industrial base. Phishing, compromised email credentials. This is oftentimes personality and personnel related, understandings people's habits and hobbies and comings and goings. Pretty simple, but this is always going to be a key part of that hacker trade craft. The second is the software supply chain. This might be a little bit overdone, but in reality, Log4j and SolarWinds are just some of the latest that we can discuss here in this type of a forum. But the fact of the matter is we have a long way to go as a nation to be able to fully secure and keep up with those supply chain threats. So that's a second key way that those hackers are going to target the design and development phase.

The third is compromising the hardware supply chain. Our weapon systems, platforms are increasingly relying on commercial components, satellite communications, telematics systems, canned buses. More and more, there are commercial entities that create efficiencies and create better data processing and speed. But many of these are also being produced in other countries outside of the United States. So in many ways this is where you can create and think about your doomsday scenario. This affords adversaries the opportunity to inject hardware back doors in certain systems, third party vendors, other nation states, other countries, a fast moving supply chain of hardware that moves into our supply chain to our weapon systems. And the ability to keep track of that and to harness those threats is increasingly difficult.

Moving further into the supply chain, we think about when these systems and platforms are deployed and operational. What do the hackers do then? Well, they conduct in theater attacks. This can be electronic warfare attacks or jamming, right? This is very common for us to deal with on the federal side and the DOD side, but it's also something that we need to think about throughout the entire supply chain. Railways, maritime, aircraft. When these systems and processes and transportation operations are in motion, that's the opportunity for in theater attacks.

The fifth is man in the middle attacks, right? This is disrupting communications, disrupting command and control and the data supply chain. One of the things that we really need to remember when we talk about the hacker is that they have a schedule too. They have a budget and they have budget constraints. So they have to operate like a business like many of us have to do outside of this room. And the other thing that we have to remember is the hackers are going to take the path of lease resistance. When you study cyber attack case studies, you'll find that the hackers are always going to look for the biggest bang for the buck, the biggest bang for the least amount of time.

And the sixth thing is maintenance. So how can hackers leverage maintenance devices to gain access? This is something that we probably don't talk enough about, but when aircraft commercial or military maritime systems, hospital systems, when they're being maintained and sustained along the way, it requires a number of IT and OT systems that keep them up and running. And that's an entirely different chain of threat and threat landscape for these hackers to penetrate.

So we think about the hacker, we think about this enormous connected battle space that we're in. The number one thing that I want to do is leave us all with some thoughts about going forward. What is it that we can do today? And there's four things that I want to hit that hopefully that you can take back to your teams and your organizations to kind of help contribute to this fight that we have. One, it's understanding your end-to-end environment. Really having a clear picture of what your attack surface looks like. What are those dependencies that you rely on to do your job? Are you in a hospital? Are you in the Pentagon? Are you in any other federal agency? What are those things that you rely on the most?

Your boundaries have expanded. What are the critical dependencies that you have and how can you maintain the best visibility of those dependencies?

The second area I want to talk about is secure by design, secure by default, okay? This is something that's appropriately highlighted in the national cyber strategy, but that's a nirvana, okay? Because the fact of the matter is we're moving towards secure by design, but we are faced with a very significant uphill battle with our technology debt. The fact of the matter is when you look at a manufacturing infrastructure or a building life cycle, sometimes no less than 20 years, so when you're looking at platforms, vehicles, buildings, you still have a 20-year life cycle dealing with infrastructure that was never built to be secure that is still that we have to operate in. So it's very important for us to support the efforts and goals around secure by design, but we got to understand that the platform and the environment that we're in is not yet secure by design.

The third is mission-based cyber risk assessments. Inside of the DOD environment, we rely very heavily on risk assessments. This can be something that you use in all of your organizations. Doing cyber risk assessments simply means taking an adversary view of your environment. What are those things that are most important to the function of your mission and how do you look at it from their perspective? If you do cyber risk assessments of any sort, that's the only way that you're going to have some idea of what those vulnerabilities are. And then you prioritize those vulnerabilities and allow you to prioritize your resources to mitigate them.

And the fourth and final area that I want to hit, which I know I'm pleased to hear that I'm probably one of many who has talked about this in this particular forum, is assume breach. Assume that attacks are occurring now. Think about resiliency. We need to be comfortable with being uncomfortable. And I'll close that out by saying we are not going to be 100% secure, but we need to be 100% resilient. So thank you very much. I look forward to any questions or continued discussion after the forum. Thank you.