Transcript, “Cybersecurity is National Security”
Episode 2 of No Such Podcast from the National Security Agency

~~Begin Transcript~~

Dave Luber: Cybersecurity is absolutely critical to national security. NSA is a combat support agency. We're supporting the warfighters.

MajGen Jerry Carter: You have sitting side by side, that is U.S. Cyber Command, with the experts from NSA, all in one building.

Dave Luber: Analysts are working the cybersecurity problem together. That's where you get to scale cybersecurity in a way that we've never been able to do in the past.

John Parker: Welcome to another episode of No Such Podcast. My name is John Parker.

Brian Fassler: I'm Brian Fassler.

John Parker: And today we are joined by two very special guests, Dave Luber, Director of Cybersecurity here at the NSA, as well as Major General Jerry Carter, Deputy Director of Cybersecurity for Combat Support. Gentlemen, welcome and thank you so much for joining us.

MajGen Jerry Carter: Thank you.

Dave Luber: Great to be here.

John Parker: We always like to kick things off by letting our guests tell us a little bit about themselves. Dave, we'll start with you. What can you tell us about your background?

Dave Luber: Hey, thanks. My name is Dave Luber. I've been with the National Security Agency for 37 years. I started very early in my career directly out of high school, joined the NSA and really enjoyed the work that we do. Also had a chance to go to school at night and earn my degrees. And over the 37 years, I've had a chance to work in a variety of missions, SIGINT, cybersecurity, and today I serve as the Director of Cybersecurity for NSA.

John Parker: Major General.

MajGen Jerry Carter: Yeah, thank you very much. Again, Jerry Carter. I enlisted in the Marine Corps in 1985. Was fortunate to get a commission through Morehouse College in 1992. So I've been serving for just shy of about 37 years. And in terms of background, signal intelligence electronic warfare officer, commanded battalions, as well as at the O-6 level. And as a general officer, had the opportunity to serve as Director of Intelligence and in various portions of the intel community.

John Parker: When we talk about cybersecurity, could you tell us a little bit about what that means to the NSA?

Dave Luber: Cybersecurity is absolutely critical to national security. So when you think about advanced cyber actors, whether it's Russia, China, Iran, North Korea, or non-state actors, it's critically important for our nation to have threat intelligence that helps us navigate all the various aspects of the cybersecurity mission. So when you think about national security systems, you think about all the systems that support the Department of Defense, all the systems that support the intelligence community, and also select portions of our federal civilian agencies and departments, also rely on national security systems capabilities. So whether it's threat intelligence, whether it's partnerships, or whether it's a focus towards key encryption capabilities to protect our most important national security systems, that's what cybersecurity means to the National Security Agency.

John Parker: Now, when it comes to cyberspace, it seems to be a very fast-moving field, particularly in the past 10 years or so. What are some of the changes that you're seeing, and why should our listeners care?

Dave Luber: Well, first off, I'd say that cyberspace is under constant change. Even as we're recording this podcast today, new vulnerabilities are being discovered, new patches are being applied to systems, critical systems across our nation, and new software is being developed by many different developers across the community. And adversaries are always looking for that advantage to find those vulnerabilities and then exploit those vulnerabilities. So, what's critically important for us is to continue to focus on ensuring that we have insights on how those adversaries are developing their tradecraft, how they're expanding their capabilities, whether it's a scope and scale perspective or the employment of new tools and capabilities. So, I think what's changed dramatically in the last 10 years is really that scope and scale. When you look at what's happening now, whether it's threats and challenges coming from the PRC or the activities that the Russians are conducting in Ukraine as well from a cyber perspective, all these different areas are demonstrating greater levels of sophistication. The other thing I think that's changed dramatically is the non-state actor community, whether it's ransomware or hacktivists. You can take a look at the example several years ago with Colonial Pipeline, where a ransomware actor shut down the flow of petroleum on the east coast of the United States and caused delays and shortages in that critical infrastructure sector. So even the ransomware and non-state actors have certainly been a big change for us in the last 10 years.

MajGen Jerry Carter: Yeah, and if I could, Dave, I think you're absolutely right. And from a military perspective, in terms of how the landscape has changed over the last decade, I would just reflect on the adversary that we were fighting. And so for the military, for the last 10 years, we were postured for this global war on terrorism. Rightfully so. It was an adversary that was not that sophisticated, did not rely on technology. And when you look at the world today and out to 2030, I mean, it's a different environment. And Dave, you hit it on cyberspace; in the past, air, land, and sea, but now we add space and cyberspace, which really challenges us.

Brian Fassler: So, Dave, can you talk a little bit more about how NSA has responded to these threats that are constantly changing?

Dave Luber: One of the big changes that we've made at the National Security Agency over the past four years is really focusing on the threat intelligence that we collect from a signals intelligence perspective, and then turning that threat intelligence into outcomes that will drive higher levels of cybersecurity for our national security systems and other critical systems across our nation. What we've learned is that we can separate what we know from how we know it, and then share that information on what we know with many different partners. Those partners can be industry partners, those partners can be foreign partners, those partnerships can also be across the U.S. government. And when you have strong partnerships with insights where analysts are working the cybersecurity problem together, that's where you get to scale cybersecurity in a way that we've never been able to do in the past.

John Parker: Now, as a newer employee at the agency, one thing that surprised me as I came in was the number of service members that work with us. Now, Major General Carter, could you tell us a little bit about the military's role here at the agency, and more specifically, your role as a senior military officer?

MajGen Jerry Carter: In my role as a senior military officer, my goal is to really sit with the technical experts at NSA, those computer scientists, those data scientists, those engineers, and help take that technical detail down to the Pentagon and translate that into requirements. Threat informed, also out to the combatant commanders, but that's a big change that we've seen in the last probably about five years.

Dave Luber: Yeah, and I'd just add to that, I mean, it is a partnership across our agency between military and civilian leaders and analysts and operators. And, you know, NSA is a combat support agency. We're supporting the warfighters in air, land, sea, space, and cyber. And it's critically important that we can speak with one voice across all of those different areas, and then ensure that we're protecting all those different critical national security systems that support warfighting activity.

MajGen Jerry Carter: And Dave, you mentioned about the partnerships and some of the key engagements that I'm responsible for from a uniformed perspective. Down at the Pentagon, some of our key interlocutors or partners are the DOD CIO, or Department of Defense Chief Information Officer. Honorable Sherman is one that I sit down with on a regular basis, advise, as he thinks through providing that best advice to the Secretary of Defense. I also say one of the key individuals that I deal with across the services is that Principal Cyber Advisor. So I work very closely with them, highlighting the threats that we see here at NSA to ensure that there are informed decisions as we translate that information to policymakers.

Dave Luber: A lot of folks think that cybersecurity is just the IT systems that everyone has on their desktop or the servers or the cloud. But in reality, cybersecurity also supports and surrounds our weapons and space systems, both current and future. So it's really important as we engage with military leaders across the department that we work together as a team to make sure that our current and future warfighting capabilities are secure.

Brian Fassler: We talked a little bit about partnerships with General Carter and the military. Can we talk a little bit about partnerships and their value to the nation as a whole?

Dave Luber: I always think of cybersecurity as a team sport. General Carter mentioned our partnership with the Department of Defense. But when you look across the entirety of the partnerships, it's throughout the U.S. government. It's partnerships with academia. It's partnerships with industry and also partnerships with select foreign partners that really helps us scale the cybersecurity mission. When we bring focus with those partnerships, we can do some amazing things to ensure that those actors that I mentioned earlier, whether it's Russia, Iran, the PRC, North Korea, and some of those non-state actors, are not successful in conducting operations against the U.S. or allied partners. So some of the key partners we work with in the U.S. government, FBI, the Cybersecurity and Infrastructure Security Agency, CISA, are a couple key partners that we're working with every single day when we think about protecting our nation from cybersecurity threats.

Brian Fassler: The partnership with the military, you know, how important has that been?

Dave Luber: One of our most critical partners in the U.S. military is U.S. Cyber Command. When you think about the work that we do between the National Security Agency and U.S. Cyber Command, it's one of those partnerships where we focus on unity of effort. While we have the intelligence mission, Cyber Command has the military mission when it comes to protecting Department of Defense information networks and also providing support to combatant commanders around the world when it comes to cyber support.

MajGen Jerry Carter: And I think that one of the things that I really appreciate and I've learned over the last year in terms of that partnership, Dave, that you just mentioned is really under General Nakasone's vision, really continuing with General Haugh, is this Integrated Cyber Center. So now in terms of the partnership you mentioned, you have sitting side by side, that is U.S. Cyber Command, with the experts from NSA, all in one building. That's a phenomenal concept.

Brian Fassler: There must be great value in sitting next to each other. Can you talk a little bit about that relationship a little bit more?

Dave Luber: Absolutely. When you think about it, we have different authorities, but when we have unity of effort, we can bring the capabilities of both partners together to really focus on key cybersecurity issues that we need to solve. So we found that bringing together the insights from the National Security Agency, the military capabilities and teams that the Cyber Command brings to bear, really brings great capability for our nation.

John Parker: So looking back, you talked about protecting our weapons and space systems. What does it look like in the future with us protecting that area?

Dave Luber: So I'll talk about space systems for a second. When you look at the changes that have been occurring across our department, especially with the advent and use of proliferated LEO, low earth orbit architectures, to support warfighters, it's been really important for us at NSA to ensure that high assurance cryptography protects all parts of that space ecosystem. So whether it's the ground segment, the user segment, the link segment or the space segment, NSA is there to support the war fighters as they develop those new capabilities to ensure that we have war fighting systems in space. So one of the

partnerships that we've had over the past three years is with the Space Development Agency. Working closely with SDA, Dr. Tournear and his team, we've ensured that over the last year, we've been able to support the launch of 27 low earth orbit satellites to support Department of Defense capabilities. And that includes the capabilities to provide secure communications from that ground all the way up to the space segment, but also bring new capabilities online to really enhance warfighting systems. And one of the things we're most proud of in the work that we've done over the past year is to have what's called Link 16 from space, command and control capabilities for weapons systems from the space sector, first ever capabilities in partnership with the Space Development Agency. We'll also support an additional 20 launches in the coming year and then more launches in the next year and years out. But that's just an example of how NSA works very closely with our US military to ensure that future warfighting systems are not only meeting the mark, but exceeding the mark when it comes to the cybersecurity aspect, but then also supporting warfighter communications.

MajGen Jerry Carter: Dave, can I just add to your point about the military and the future systems? The thing that we see today is the development of artificial intelligence, machine learning, and how we, the capability can really give us a decision advantage on the battlefield. So I spent a lot of time with my counterparts in the services down at the Pentagon, ensuring that they embrace that technology, but it's in a safe and secure way. I've learned a lot of things by serving in just a few months at NSA on what NSA is doing in that area. Dave, any thoughts about artificial intelligence?

Dave Luber: Absolutely. You know, six months ago, we set up our AI Security Center within the National Security Agency, and it has three main objectives. First, detect and counter foreign threats that would impact AI systems that we would want to use in our national security systems. The second is to really focus on developing deep partnerships, deep partnerships with industry, deep partnerships with those across the national security community that would want to use and implement AI for either warfighting capabilities or intelligence community capabilities. And then the last is really to develop and promote best practices in securing AI. If you take a look at one of our cybersecurity advisories that we published on 15 April, you can find this on NSA.gov, but it focuses on how to deploy AI systems securely. It's one of our first publications that we worked on with CISA, FBI, our teams here at NSA, but then also our Five Eyes partners across the community to make sure that we were promoting that AI security guidance. There'll be more publications to come in the future.

Brian Fassler: I was going to say, can you tell us a little bit more about cybersecurity advisories? Where do people access them and how do they leverage them?

Dave Luber: Well, first off, you can access all of our cybersecurity advisories at NSA.gov. And really, the cybersecurity advisories are curated and focused insights to take threat information and then drive systems owners and network defenders to the priority items that they should focus on to protect their systems. And while they're focused for the national security community, they're also applicable across our critical infrastructure and industry systems. So really, these advisories can be used for many different systems owners out there.

Brian Fassler: And you also stood up the Cybersecurity Collaboration Center, where I imagine a lot of those relationships are also leveraged. Can you talk about that a little bit?

Dave Luber: The Cybersecurity Collaboration Center is our unclassified area for which we can engage with industry on a regular basis. And really, the power of those partnerships is at the analyst level. When analysts from NSA and analysts from industry, especially the Defense Industrial Base, can focus on what we see in cyberspace and what we see from those advanced cyberactors, this is where the power of partnerships between industry and government really comes to focus on those particular threat areas. So it's been a tremendous game changer for both industry and government and has allowed us to really scale the cybersecurity mission.

MajGen Jerry Carter: I think from a military perspective, why is that important? Because we really rely on many of these industry partners to build some of the capabilities that we're going to use, not only in competition, but in conflict. So, going back to earlier discussion about why is cybersecurity important and why is partnership important? I think you absolutely nailed it, Dave. Thanks.

Brian Fassler: And it sounds like it's a two-way communication channel, right? It's not like NSA is telling everybody else what to do, but we're learning from private industry. They're bringing to the table intelligence or insight that we as a government agency might not have.

Dave Luber: Yeah. Let me give you a great example of that. In May of last year, we worked on a hunt guide that allowed national security systems owners and critical infrastructure owners to identify PRC cyber actors that were using normal command line techniques, normal operating system commands, to penetrate critical infrastructure systems and other U.S. government systems. And what was critically important in getting that hunt guide together was the partnerships with industry. So if you take a look at that particular publication, there's over a dozen industry partners acknowledged in that publication that contributed to the insights that allowed us then to promote and push that guidance out for national security systems owners and critical infrastructure systems owners to go and protect their systems.

John Parker: Now, looking to the future, say the next five or 10 years, where do you see the agency?

Dave Luber: So some of the key cybersecurity areas that we'll be focusing on now and into the future: really focus on first, development of the workforce. I spoke to that just a little bit ago, but it's really critically important that we continue to develop the future ready workforce in the cybersecurity arena. Second, there's different ways that we have to think about protecting our national security systems. So in the past, we would think about protecting national security systems with perimeter defense capabilities. But if you take a look at the activities that were just the last year since January, there's been nine major vulnerabilities discovered in perimeter defense systems. If that's the only way you're protecting your systems, that's not a good plan. So what we really have to think about is Zero Trust. And Zero Trust considers that a breach will occur in your systems. But the concepts and methodologies behind Zero Trust focus on the idea that you can monitor and segment the networks in a way that ensure that if the perimeter or if the systems are breached, that the adversary has limited capability to move within that system to pivot to the critical data that you're trying to protect. So as we work with the Department of Defense and the IC to develop guidance and zero trust systems, that's one of the key things that we're working on with the community. The other key area that we're focusing on is ensuring that we have quantum resistant cryptography to protect our national security systems. And a quantum

resistant crypto roadmap really allows us to ensure that if the Russians or the PRC have a quantum computer in their hands in the future, that our cryptography will be safe from being exploited by that computer. Of course, that partnership goes across the department, the IC, but we also work very closely with the National Institutes of Standards and Technologies, NIST, to ensure that the rest of the community is also protected from the quantum threat. So NIST is really critical because it's not just NSA that focuses on quantum resistant capabilities. We also have to make sure that industry, other parts of government, are also protected from the quantum threat in the future as well.

MajGen Jerry Carter: And I would say from military perspective, we talked a lot about partnerships and the value of partnerships. We'd like to continue to see the strength between the NSA and the military partnership. In fact, I would just say the department is thinking very hard about growing that capability. No daylight between the two, side by side, for all the right reasons that we cited. And then in terms of the future, each of the services are going through a modernization effort. In Marine Corps, it's Force Design 2030. And as we think about tomorrow's adversary and tomorrow's fight, Dave, just brings it back to the things you highlighted. Safe and secure communications, and that starts with modern and resilient cryptography. But all those things are pretty important for tomorrow's fight.

John Parker: So as we wind things down for today, are there any last minute takeaways that you'd like to share with our audience?

MajGen Jerry Carter: The cybersecurity and importance to the military, I mean, it's a big deal. So I've learned a lot since being here at NSA. And the thing that I'm completely focused on is ensuring that we have that resilient and ready workforce. Not only changing the culture about how important cybersecurity is, but ensuring that we're building the next generation of leaders, warfighters that not only understand cybersecurity and its importance, but really embrace it, on the cutting edge of this new technology.

Dave Luber: General Carter, I can't agree with you more because when I think about the people of the cybersecurity mission, that's the most important part of NSA. That's the most important part of what we do between NSA and the partnerships with the Department of Defense and our military. We take the development of our teams seriously. And it doesn't just start when you join NSA. If you think about the partnerships we have with academia, the Centers of Academic Excellence, as an example, we have over 470 partnerships with universities across our nation to help ensure that the next generation of cyber experts are getting the training, getting the insights that they need to then come join the US government. So whether it's cybersecurity, cybersecurity research, or computer network operations, the partnership with academia helps ensure that we're prepared not only for today, but also for the future so that the next generation of workforce comes and joins.

MajGen Jerry Carter: Dave, I can't help but as you give your comments about this ready workforce, just recently we had an opportunity to celebrate one of our teammates in the cybersecurity directorate. He was a high school work study. He joined us for the summer program, graduating this spring and heading off on a full ride scholarship thanks to the Department of Defense. That's exactly what we need to do to build this ready resilient workforce that really understands the technology of the future for tomorrow.

Dave Luber: I like to think of it as working left of launch of a career. And when you can focus universities, when you can focus even K through 12 development through programs like GenCyber, it begins to present opportunities for students to get involved in STEM, get involved in cybersecurity. Think about cybersecurity as a career so that when they do decide to join NSA, FBI or CISA, they're ready to support our nation.

MajGen Jerry Carter: Yeah, fantastic.

John Parker: Dave, Major General Carter, I'd like to thank you both again for joining us today. It's been an honor. Once again, my name is John Parker.

Brian Fassler: I'm Brian Fassler.

John Parker: And this has been No Such Podcast.

Cam Potts: Thanks for watching this episode of No Such Podcast from the National Security Agency. If you enjoyed the show, please leave us a review and make sure you're subscribed so you don't miss our next episode. For show transcripts and other information, please visit NSA.gov forward slash podcast.

~~End Transcript~~