Transcript, “AI and the Future of National Security”
Episode 3 of No Such Podcast from the National Security Agency

Vinh Nguyen: AI has been embedded in our society and our technologies for decades.

Tahira Mammen: The AI of last year is not the AI of today and will not be the AI six months from now that we think about when we think about national security challenges.

Vinh Nguyen: This is an evolution in technologies and we need to harness for national security.

Cam Potts: Welcome to another week of No Such Podcast. I'm one of your hosts, Cam Potts, alongside my co-host.

Brian Fassler: I am Brian Fassler.

Cam Potts: Yes, and we're here to talk about the evolutionary technology, artificial intelligence. That's right, AI. What is it? What does it mean to national security? But more specifically, what does it mean to the National Security Agency? Well, today we are joined at the table by two of NSA's subject matter experts, Ms. Tahira Mammen of NSA's AI Security Center and Mr. Vinh Nguyen, NSA's chief responsible AI officer. Thank you and welcome to No Such Podcast. All right, so we are here at the table to talk about AI. Vinh, could you take us down the road of what is AI? Is it here to stay?

Vinh Nguyen: Well, AI is definitely here to stay and we've been using AI and you all have been augmented using AI that you don't even know. You are using AI for like a decade or more. But AI has been kind of like, you know, sprinkling in the background and it's like technical, people don't pay attention to them. But since last year, we have generative AI and various chatbots, you know, coming out and now it's in your face and now you're like, oh my God, AI is here. But AI has been embedded in our society and our technologies for decades. But when you really think about AI and the way we think about this, is that really is a frontier of automation. We’re quite comfortable with automation, right? We have done this since the 18th century. We automate, right, as we go. And now we, you know, as a human society, we have this opportunity to automate a very special set of activities. And this is quite unique, right? It's automating the way we see, the way we hear, the way we comprehend languages, the way that we reason. Now that sounds scary, but researchers have been working on this for a long time and we have been embedding AI in all facet of our lives already. So, you know, I would say this is really about automation and NSA has been a leader in integrating, you know, these technologies into our mission. And so there's nothing to fear. This is an evolution in technologies and we need to harness for national security.

Brian Fassler: Since you've referenced the 18th century. So that means that it's probably changed a lot over time right, I mean, I probably take advantage of AI every morning when I'm, you know, wanting to know what the weather is, when I want to know how to get to work. So, you know, tells me what traffic to avoid, things like that. And I think one of the, to my understanding, one of the base principles is like, it's only as good as the data that is captured. So can you talk a little bit about the data that's being used and the importance of making sure that it's all encompassing and what happens if you don't have the accurate, you know, data in your data set?

Vinh Nguyen: Right. I mean, at the core of the technology is really about quality data. And so, yes, you know, we all have algorithms, we have compute power. But at the end of the day, you know, the power to bring AI machine learning to bear for our organization is the quality of the data. And so, you know, we cannot just use, you know, any AI. We have to make sure that we have the right data that is, you know, legal and compliant and privacy preserving to really deliver on what exactly we want to achieve. And so, data is really key. And I think a lot of time, you know, people don't talk a lot about it outside of, you know, some AI application. But here at the National Security Agency, we really care a lot about the quality of the data. How do we harness it? And how do we protect and secure it?

Tahira Mammen: Yeah, I would say from the cybersecurity perspective, that the quality of the data as Vinh is saying is so important, but also making sure that we maintain a focus on protecting it because your data is only as good as the security mechanisms that you have around it, right?

Cam Potts: I think that it's great to hear compliant and safe when it comes to implementing this technology and having this as an available thing and something that the agency is in the forefront of leading.

Vinh Nguyen: Oh, absolutely. AI is actually not new to the agency. For those who don't know, and for the audience, you may not know. But you know, the National Security Agency had been working on AI and machine learning since AI started back in the 60s. So, you know, this is a very mathematical, you know, like deep math work that NSA had been involved with. So it's not like new to us. We have a long history of doing this. We understand the potential, but we also understand the risk. And so we are taking a very, you know, set of measures, steps to really do this right and do it in a responsible way.

Cam Potts: So we can't be the National Security Agency and not talk about the national security challenges that AI may pose. So Tahira, could you outline what some of those challenges are?

Tahira Mammen: Sure, I would say there's two things that we really looking at, right? First is the pace. The pace of capability development that we see, right? The AI of last year is not the AI of today and it will not be the AI six months from now that we think about when we think about national security challenges. And the second is the scale, the scale of implementation, the availability of AI in the public, and then specifically with our foreign adversaries. The way our foreign adversaries are advancing their capabilities with pace, where our foreign adversaries are scaling, right? Implementing and what that means for our national security. And especially this year and in election year, election security and the role that AI has to play there is a key focus for the National Security Agency.

Vinh Nguyen: Yeah, so I think it's a challenging time, right? In term of we see China as a pacing threat, as a strategic competitor. And, you know, when you look at the PRC or the People's Republic of China and the government, they're very focused on investing in AI to gain that economic, diplomatic, political and military advantage. And so they see AI as a core technology and a core opportunity for China to grow and out-compete and outmaneuver, outmatch the United States and the West. So it's quite challenging. We do not want to live in a society where our AI are built, run by the PRC. Because they are not built on our democratic values. And so we have to think strategically on the national security implication of that level of strategic competition. Now, you know, at a more obvious level is that, like Tahira mentioned, is that adversaries are investing, using, exploiting the technologies so they can embed them into military weapons, right, to disinformation campaigns, to cyber operations. My assessment is that the national security threats that we're facing are just being amplified by AI. You know, when you see not only nation

states, but also non-state actors are using AI to, you know, including cyber criminals, right, to run their campaigns. So we are seeing the amplification in terms of the scope and maybe the consequence of the threats. And so we have to really understand how this threat is manifesting and also how to manage the risk. And especially, you know, how can we manage the risk of foreign cyber attacks against our own mission capabilities, national security systems, and weapons systems. We need to secure the systems to maintain that advantage.

Tahira Mammen: I think the proliferation of generative AI capabilities, right, just out and available to the public, we've already seen how that has an effect on non-nation state actors being able to leverage it in ransomware, in cyber criminal activity. Most of us have probably heard in the news about different audio, video, you know, synthetic media generated to sound like somebody you know, or somebody you trust, or someone in leadership that helps cyber criminals, you know, reach their, usually, financial aims, right, but not always, right. Disinformation campaigns can have wide reaching impacts and AI presents capabilities which have great power for good, right. But in the cybersecurity landscape, we also have to be looking at how they can be used for deepfakes, right.

Brian Fassler: In terms of the disinformation, it's an election year. NSA has had a role in ensuring that our elections are secure. Can you talk a little bit about, you know, what are we doing in 2024?

Vinh Nguyen: Absolutely. You know, this year, you know, people are talking a lot about AI, because we know that, you know, our adversaries, you know, state and non-state are leveraging generative AI to influence or aiming to influence our election. NSA working with our US government partners are really, you know, trying to deliver our, you know, exquisite intelligence insight that we can get to secure our election, work with the partners so that we can bolster countermeasures and ensure, you know, ensuring that, you know, our elections and our infrastructure is safe and secure for the American public.

Cam Potts: Seems like the power of partnerships is the superpower here. And without it, we're not able to be effective. But with it, we're even better. So in the topic of election security, Tahira, you mentioned the pace, talked about the scale. With the AI Security Center, former DIRNSA, General Paul M. Nakasone stood up NSA's AI Security Center in September of 2023. It's now stood up. It's now in forward motion. Now this center, the center that you lead, what is the AI Security Center doing to keep our country safe?

Tahira Mammen: The AI Security Center, keeping in mind, right, the responsibility to secure national security systems in the defense industrial base, and to enable them to be using cutting edge technology, right, in a secure way, because that's really what we have to do for all of national security systems who'll be accomplishing their mission, right? AI is a critical component of the technology that they need. And NSA and the AI Security Center, we aim to provide the security, the best practices that they need so that when they're implementing AI, they know that they're doing it with security at the forefront, right? We have just stood up, hit IOC at the end of December, initial operating capability. And, you know, what we're really trying to do is get information to our customers in the national security systems in the defense industrial base about how to secure their AI as they're implementing it, right? I think if you think about the history of the internet, for example, right, we like make the internet and 10 years later go, hey, we should encrypt some stuff. Or hey, let's, how about certificates? And so, you know, AI is rapidly expanding, rapidly growing just within society, right? And security, we know better now, right? We know that security needs to be at the beginning at the implementation phase of that. And so we in the center seek to understand the threats given the like exquisite insight and intelligence that NSA has across its two missions, SIGINT and cybersecurity, to take that information and connect it to researchers that work

within our center who are brilliant. And now we're doing that work to take those insights. And when we can get them to the right classification level to have engaging information exchange with industry who's creating, running, right, delivering these solutions to the national security systems. Because that's how we inform the researchers on what the threats are, right? What the capability is and what we need to do to secure it. And when we get all those pieces lined up, and then the delivery is best practices, right? NSA says this is the best practice for deploying your AI. This is the best practice for your model security. This is the best practice for access management and authentication, right? And so we're getting our feet under us right now. And then what the year looks like for publication.

Cam Potts: Awesome. And you talk about mission and how potentially AI can be used in that area. Can we potentially get into maybe an example of how AI was used in a mission success here at the agency?

Vinh Nguyen: Yes, absolutely. And I think it's, you know, not just for intelligence, but, but, you know, using it in cybersecurity, of course. And so, you know, for those who may or may not know, NSA has two major missions. One is to deliver foreign intelligence through signals intelligence, and the other one is cybersecurity. And for foreign intelligence, we have been leveraging AI machine learning for decades, like long, long, long time. Just imagine, you know, the work that our analysts do, right? How can they understand, you know, foreign leaders, you know, speaking, and their planning, and what, you know, foreign militaries, you know, are up to. We all communicate. That's the point of signals intelligence, meaning that we also have to understand what we hear, what we see, and also how we comprehend languages. You can see AI allows us to do that, you know, through machine translation. What we found was that AI can be embedded through the entire intelligence analyst workflow. And then we insert AI to augment every step of the way. And so we've done a lot of this work, and we, you know, don't shy away from it.

Brian Fassler: Can you talk about the authorities that are in a place to ensure that we're using AI responsibly?

Tahira Mammen: I think one of the most important responsibilities that we have as a cybersecurity mission in NSA is helping to protect the national security systems in the defense industrial base, right? The director is the national manager for those systems, and so in the cybersecurity directorate, which is where the AI security center is located, that is a primary focus for us, right? And so national security systems, our weapons and space platforms, and any network that has classified information on it, so you know, our nation's top secrets reside on these networks. And in the cybersecurity mission, we seek to provide the cybersecurity for those. As technology advances, right, and AI becomes a part of what NSS owners or the defense industrial base wants to implement into their networks, then security of those AI systems becomes really important for just comprehensively working towards our shared security.

Vinh Nguyen: Yeah, I want to add what Tahira mentioned is, you know, we have a lot of discussions in terms of protecting privacy, security, safety, and whatnot, but at the end of the day, like, AI security is really fundamental and foundational to protect everything above. You know, a lot of times people will say, "Oh, AI safety, AI safety." That's okay, but if you cannot secure your safeguards, you don't have any safety. A good example, you know, that I can think about would be like a stop sign, right? Or, you know, if it's more dynamic, it's, you know, a traffic light, right? A traffic light is a safeguard, right, to ensure that we drive safely and prevent accidents. But if you think about it, if the traffic light is not secured and hackers can hack the safeguard, then you actually have no safeguard. You have a beautiful traffic light. And traffic everywhere. And you have the traffic light, it doesn't do you any good. So, I think that is like

how, you know, we think about security is so foundational. When the nation talks about safety, and we recognize the many opportunities and challenges of AI safety and the potential of a harm that could cause to users by AI. But we want to also understand that in order to have the safeguards, we also have to secure them as well. And so, we're working with literally everyone trying to figure out how to help the nation on that front.

Cam Potts: Awesome, awesome. Now, I know we can talk about artificial intelligence, we can talk about AI all day. And even while we're talking right now, during this podcast, the technology itself is advancing. So, to actually wrap this up, I would like to go into talking about AI in the future, where it's headed. And what do we see? Is society prepared for where AI is headed as a technology? Vinh, we'll start with you.

Vinh Nguyen: Yeah, absolutely. I would say that we cannot really, you know, tell you like what fancy technologies will be popping up. But what I can tell you is that NSA, you know, is watching this space very closely to understand the opportunities, but also manage those risks that we see, especially AI security.

Tahira Mammen: Right, when you say, you know, are we ready, that is the mission of the AI Security Center. It's for national security systems to be ready and secure as they implement AI technologies. So, we're doing all that we can at NSA and within AI Security Center, investing our resources, our people, our expertise, and bringing what we have to bear as NSA to the problem.

Cam Potts: Well, thank you so much for sharing that. I must say, while we may not necessarily know for sure what will happen, at least we know that we have professionals in our NSA subject matter experts working in partnership with other industry and other experts to just counter the measures that come with this technology and where it's headed and what's going to take place. So, if someone wants to work within the mission of AI at the National Security Agency, where should they go to actually see about those opportunities?

Vinh Nguyen: Yes, go nsa.gov. And we have a series of AI jobs that you can apply to, AI engineers, data engineers, MLOps engineer, data scientists. Feel free to link up and our team here will be in touch with you.

Tahira Mammen: Yes, and I would say that NSA has a really robust program of internships for college students and even high school interns where, you know, who's on the cutting edge of technology? Usually college people, right? And so, those applications usually run in the fall, but all available on nsa.gov. And a really, really important way that we bring talent into the agency and new ideas, right? Because you have to have sort of an innovative mindset to be doing AI security work. And we are interested in those people.

Cam Potts: Well, high school students, college students, you have heard it here first, the opportunities are available for you for internships. And of course, for anyone else, you can head over to intelligencecareers.gov/NSA. Is there anything else you all would like to share with us today?

Tahira Mammen: I would add that anyone that's interested in the work that happens at NSA, cybersecurity is the place where you can learn a lot about what we're doing to defend our nation. So on NSA.gov slash cybersecurity, you can find the cybersecurity products that we put out about what the adversary threat looks like, how to secure your network, how to do zero trust, how to do cloud security.

There's a ton of great content there, including some AI security center publication about secure and resilient deployment of AI systems. So recommend everybody check us out.

Cam Potts: All right. Well, Tahira, Vinh, thank you so much for joining us today on No Such Podcast. It's been a pleasure to have you here with us to talk about artificial intelligence, where it's headed, and what the agency is doing to get at the forefront of this technology. Thank you. Yes. All right. Thank you for joining us. It's been a pleasure being your host for this episode. My name is Cam Potts alongside my co-host Brian Fassler. All right. And we look forward to seeing you next time on No Such Podcast.

Ending voiceover: 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~~