Delivering Next Generation Cyber Capabilities to the Warfighter

Featuring Greg Touhill as Interviewed by Matthew Butkovic

Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

Matt Butkovic: Welcome to the SEI Podcast Series, a production of Carnegie Mellon University's Software Engineering Institute. My name is Matthew Butkovic. I am the technical director for Cyber Risk and Resilience in the CERT Division of the Software Engineering Institute. Today I am joined by General Greg Touhill. Welcome, Greg.

Greg Touhill: Thank you, Matt.

Matt: Greg is the director of the CERT Division of the Software Engineering Institute. We are here to discuss the work of CERT. Before we get to that, Greg, I would like to round out your bio. Greg is a 30-year combat veteran of the United States Air Force, where he was an operational commander of the squadron, group, and wing levels. After his retirement from the Air Force, Greg was appointed as a Deputy Assistant Secretary for Cybersecurity and Communications in the Department of Homeland Security, DHS, where he led national-level programs to protect America's critical infrastructure. Later,

he was appointed by the president to serve as the first chief information security officer, CISO, of the United States government. Prior to his appointment as the head of the CERT Division, Greg successfully served in several leadership roles in industry, including as a board director who led two startups through growth to acquisition. He was also on the advisory board of three Fortune 100 companies and was the president of a cybersecurity startup. In addition to his role in the CERT Division, he is also an adjunct faculty member of CMU's Heinz College. Greg is also an accomplished author and a senior executive with high levels of access on the battlefield and in the boardroom. Welcome, Greg.

Greg: Thank you.

Matt: Greg, you bring a wealth of experience across a really interesting cross-section. You are a combat veteran, a senior military officer, a senior leader in government, and a senior leader in industry. I think you are well positioned to have a discussion about how the SEI—and in this context, CERT—is adding value to the Department of Defense and better equipping our warfighters. Recently, the secretary of defense described reviewing our mission readiness in regard to cyber, and its joint operations in many forms. As an opening question, Greg, your thoughts about how the SEI broadly and CERT in particular add value to the missions that matter most to the secretary of defense and the Department of Defense?

Greg: Well, thanks, Matt. First of all, I think every single secretary of defense during my long career, which spans back to when I enlisted on September 6th, 1979, every single secretary of defense as they come in, they are going to establish a comprehensive review of the current state of the Department of Defense. I think it's very encouraging that this particular secretary has put cyber at the top of the agenda. Taking a look at the Cyber National Mission Force is fair and appropriate given the environment that we have in cyberspace. Our national security and our national prosperity are heavily reliant on a safe, secure, and trusted cyber environment. And, as a result, organizations like ours, the Software Engineering Institute and specifically the CERT Division of the institute, are critical for the nation and have been since the inception of the institute 40 years ago in setting those best practices, conducting the innovative applied research and development activities, yielding new capabilities to make not only the internet and the cyber domain safer, more secure, and more trusted, but also setting the conditions for new technologies to leapfrog forward, such as what we are seeing now with artificial intelligence and machine learning. You have heard me say artificial intelligence is an overnight sensation that was over 65 years in the making. I

think at this pivotal point in our nation's history, the Software Engineering Institute is needed more than ever to help make sure that national security, but also national prosperity is preserved, protected, defended, and we increase our capabilities and our advantage in marketplaces and make the lives of our citizens even better. We increase our capabilities and our advantage in marketplaces and make the lives of our citizens even better. We increase our capabilities and our advantage in marketplaces and make the lives of our citizens even better.

Matt: Thanks, Greg. I think you are making a very important point that when we when we speak about the contribution we make, it certainly is in direct support of national defense but also national prosperity. When I think about homeland security and critical infrastructure, this is distinct from DoD missions, but certainly related. In my mind—certainly you raised your hand in 1979 to defend the nation—a host of new technologies and new threats have emerged, as you mentioned, regarding artificial intelligence will continue to see the addition of technologies that provide both opportunity and a new source of risk. I would like to spend just a moment talking about the join between the things that we do for our federal mission partners, like Homeland Security and the Department of Energy, and the things that we do for the Department of Defense.

Greg: Well, you can't have the military doing its job without the critical infrastructure that underpins the fabric of society. As commander of an installation, and I was a base commander, we had 18 C-130s on the ramp, 4 C-21s. We were training 12,500 airmen at a time through our technical training programs. It was a large installation. I even had the third largest hospital in the military on my post. As you take a look at that, I was reliant on critical infrastructure to execute my mission to launch airplanes. The hurricane hunters couldn't fly if we didn't necessarily have all that critical infrastructure that was provided off base by public utilities, by water companies and such.

One of the things that I fell in love with at the Software Engineering Institute is the fact that that research that we were doing sponsored by the DoD is complemented by the research we do for federal civilian executive branch agencies and departments that are focused on that critical infrastructure. Much of the research that we do is applicable to both. A great example is some of the stuff that we have been doing for the Department of Homeland Security and looking at how to better secure federal civilian executive branch networks. How are we working to better secure critical infrastructure? We have done some really amazing research, for example, in better insights in

cloud telemetry. As we go to a hybrid cloud model where you have multiple vendors that are out there, how do you determine whether or not you are optimized to make sure that you are safe and secure in those different clouds and the people's data, the citizenry data, is protected? Well, those same concepts that we were doing for DHS, and the lessons learned from there, we were able to apply in the Department of Defense as well as sharing with Joint Force Headquarters DODIN [Department of Defense Information Network] and the folks that are working on the military networks and the application in cloud architectures. And the results are pretty profound. The network situational awareness teams that work for you, they delivered a 50 percent storage optimization improvement in an AWS environment. As you take a look at Azure, 20-to-30 percent improvement. That is capabilities and improvements that helped save taxpayers money because it reduces waste, but it also provides greater insights for the operators there. As a military professional, I want to be able to outthink, outsmart, and out act our adversaries. With those types of improvements that our researchers are able to provide, we maintain a competitive advantage not only on the military standpoint but conveying that to our industry partners, we maintain a competitive advantage in the marketplace as well.

Matt: Thanks, Greg. That convergence, I think is really important to understand. You and I both transitioned from industry to the SEI. It gave me an opportunity to do something more meaningful for national defense and national prosperity. It allowed you to take up that banner again in a more direct way. I think one of the things I am most proud of is that we are finding those points of intersection between industry and academia and taking that value back to the DoD. I am very proud of the work of the team that is doing cloud telemetry. It seems to me the infrastructure the DoD is depending on is increasingly looking like the commercial infrastructure that you and I knew in private industry. That transition of best practices, of safeguards, in a way that is fit for purpose for DoD, cost effective, scalable is really important. I am very proud of what we have done there. Another area I was hoping we could explore is the work we have done in understanding incidents related to AI systems, responding to them.

Greg: Absolutely. We are very excited about the work that is being done by our Artificial Intelligence Security Incident Response Team, or AISIRT. That is actually a team that is focused primarily here in the SEI. Actually, we leverage our vast network of friends. We have not only the foundational researchers on campus that we collaborate with, but also within the SEI, across the tech divisions here, we are leveraging all of the experience from our Software Solutions Division, our Artificial Intelligence Engineering teams, as well as the

full CERT team in taking a look at all these different vulnerabilities that we are seeing being reported to the CERT as part of our mission as the CERT Coordination Center for the whole world. Back in 2023, we stood up this AISIRT because the volume and the severity of the different vulnerabilities involving the artificial intelligence ecosystem was continuing to rise. Some of those vulnerabilities that were being reported were pretty alarming. Examples of things that we continue to see, and we have coordinated well over 100 over the last year including vulnerabilities associated with the models that are foundational to the creation of AI systems. We have seen vulnerabilities injected into the data that is used to train models. We have seen vulnerabilities in the supply chain of the GPUs, the chips that are used to power and fuel the AI machinery, so a supply chain issue there. Then we have also seen other vulnerabilities in the ecosystem, which, it touches every aspect. The hardware, the software and the wetware, the human elements as well. All three come together to form those AI systems. Our position here at SEI, we have nearly 40 years' worth of experience in CERT coordinating vulnerabilities, sharing vulnerability information, as well as how to mitigate them, serving as what I like to call the cyber neighborhood watch. AI systems are part of that cyber ecosystem. They rely on hardware, software, telecommunication, networking. All the aspects of cyber are encompassed in AI systems. I am a big fan of Star Trek as you know. I like Kirk and his crew, but I also like Picard in *The Next Generation* and his crew. CERT was founded in the first generation, the original. Now we have moved to the next generation, but the mission is the same. AI vulnerabilities or cyber vulnerabilities, and we are a centerpiece in the ecosystem for making sure that if we see something, we say something. We have a collaborative network of, over 4,000 contributors. We are raising the bar, raising awareness, and helping AI be as good as AI can be, as safe as AI can be.

Matt: Thanks. Great. I think that is one of the through lines in our history. And again, another reason to be very proud of being a member of this organization. When posed with the challenge of thinking about AI vulnerabilities, we didn't start with a blank piece of paper. We are drawing on this long lineage. In many ways, being the first to offer these sorts of solutions when CERT was established in the late 1980s. I think about incident response, vulnerability analysis, insider risk. We are drawing on a corpus of cases and incidents to analyze and also a long-established catalog of best practices and metrics. I think that is one of the things that demonstrates unique value for this institution to the DoD.

Greg: Well, and we have been working with industry on these vulnerabilities and having a positive impact. For example, we got a report of a jailbreak

vulnerability, which basically means there was a vulnerability that allowed an attacker to bypass the guardrails within the AI system. If you bypass the guardrails, you can do a couple of different things, including being able to tamper with the system that would cause it to guess a wrong result or being able to elicit data that you shouldn't be allowed to see. So, we worked with the vendor and were able to make sure that that vendor corrected that problem. We showed them, *Here is what the problem is. Here is what the implications are. Here are some suggestions on mitigations*. The vendor worked really, really quickly to handle that.

Another problem that we worked at with some profound impact was on a situation we call leaked locals. It is basically a memory leakage within the computer systems that power AI. Our researchers were alerted to and researched where the memory leakage was. It was a situation. We have seen it in the traditional cyber world back in the original series, but now we are in the next generation seeing that memory leakage in AI systems. That was bad, where it basically said, *OK, if I have leftovers, I can go and see what the previous question was. I can go and be able to provide surveillance on the use of that model in the past, and I can use that information to figure out how that model works, and then I can go attack it.* We went to a vendor that we were seeing this vulnerability being exploited in and talked with the vendor, showed them how to fix that. One of the things that we do, and we have built on this over the last 40 years, is we don't punish the victims. We anonymize. People can come to us, we help facilitate the repair, what to do about it, and then we share within an anonymized manner, unless that company wants to come forward or that military unit wants to come forward or whatever. You never punish the victim, you just try to make the ecosystem better.

Matt: I believe, Greg, that is how you build the trust required to have the substantive dialogue that we need with industry. I think another unique element of our value proposition is being that trusted agent in these conversations among our stakeholder set.

Greg: Absolutely. While most of the work we do is at the behest of the Department of Defense and federal civilian executive branch agencies, we can also work with companies themselves. If the companies are seeing a gap, and they say, *Hey, I really could use the insights from your experience, research teams*. We can in fact, go do work with them. We are in negotiations right now with a major Fortune 10 company that is concerned about how AI and humans interact. They are asking us for help in getting better insights from an insider threat perspective on the employment of AI, robotics, and human elements into the critical manufacturing of devices that they bring to market.

As we take a look at the research and engineering landscape, we turn science fiction into reality here at the Software Engineering Institute. We do that primarily for government and the military. We want to make sure that our industry is as competitive as possible as well, and we share our lessons as much as we can.

Matt: I like the phrase you use, which is turning science fiction into reality. Now I don't know Star Trek as well as you do. I am not sure this is a correct assertion, but after the next generation, there is another generation of Star Trek. Is it Captain Riker? Is that correct?

Greg: Oh, Riker is already a captain. I think he has been promoted to admiral since the last Picard series. But now, actually, Seven of Nine is the captain of the USS Enterprise-G.

Matt: Apologies for not for not knowing that. Let me explain why I asked it that way. You described the founding of CERT, the next generation. We will have a next generation of the next generation. The question that I have for you is which technologies, which new sources of risk and reward should we be thinking about as we put a 5- and 10-year horizon on that question?

Greg: As you take a look at a technology…Technology is going to move forward. We want it to move forward. We are Americans after all. Our country was built on change and moving forward. We embrace new technology. We want new and improved. It is just built into the fabric of our society. Every generation should be looking at improvements. That is really where it boils down to. As we take a look at it from the cybersecurity standpoint, the initial cadre of folks here that created CERT in response to the Morris worm incident back in 1988, they really birthed not only the discipline, but [their response to that incident] led to the spinoff of all those things that they learned into a whole industry. Where we are right now is, generative AI leapt off of the drawing board and into the boardrooms rather quickly with the advent of OpenAI and that model being made to the public in a pretty easy web-based front end. That, like I said, is the culmination of 65 years of research. There is research that is ongoing that is going to take us to that next big thing. As we go and try to forecast that next big thing, there are going to be some foundational elements that lead to that, and some things never change. When it comes to the cyberspace domain, we ultimately want to provide results that are effective, efficient, and secure. Further, from a societal aspect, as we move forward with things like AI and the vast amount

of data that it consumes and the transparency it can provide, we will still want to safeguard essential elements of our societal compact of privacy, civil rights, civil liberties and such. I think the next generation is going to create some fantastic research that is already being explored in the labs here at Carnegie Mellon and in other places. But those foundational rules we live by—the scientific method, the rigor and disciplines, the peer reviewing, the methodologies—are going to stay the same. Further, the values and the ethics that we bring to our research are going to remain the north star for us to continue to follow.

Matt: I think that is a great point Greg. All of these things require an overlay of governance, and the fundamentals are perennial. The things we advocate at the base level of risk reasoning, ethics, and making sound decisions based on data and evidence will persist no matter what. So, in five years, if you and I are talking about quantum or synthetic bio, chemical computing, whatever it may be, I believe one of the other values we add as an institution is providing those perennially important elements of understanding these big challenges.

Greg: Yes. That is really one of the values of research institutions like we have and that we belong to. Those values, the discipline and rigor, all of those things were attractive for me. I was a consumer of the different revelations that SEI brought in software engineering and cybersecurity. Throughout my professional career, from my military into government and into industry, I relied on the SEI to help lead the way and shine that light forward so that I could see what is within the realm of the possible. That is one of the great values of the Software Engineering Institute in shining the light onto the possibility of different things. As we go and we take a look at making science fiction, turning it into reality through some of the work we do, and inspiring the work of others to make it so, we want to make sure that we are well anchored in that scientific discipline and the rigor that goes behind it. Once we take a look at AI, for example, it is exquisitely complex. You want to have things like explainability, you want to be able to say, *Well, how did you come up with that?* You don't necessarily want to have just a black box. You want to have the ability to make sure that some of these new, amazing technologies…It is not just an invisible, *trust me* black box. You want to make sure that we have the capability of making sure that that computing is, in fact, trustworthy, it is explainable, it is reliable, and it is also responsible,

Matt: Verifiable confidence in these things. Now, Greg, I am extremely proud of you. Part of your team and part of this, this institution, and the unique contribution we make, to the warfighter, to our partners and other elements of government. Certainly, I look forward to where the path takes us. Thank you so much for joining us today for this conversation.

For our audience, we will include links in the transcripts to the resources mentioned today. Finally, a reminder to our audience that our podcast are available on SoundCloud, Spotify, Apple Podcasts and the SEI's YouTube channel. If you like what you are seeing here today, then give us a thumbs up. Thank you for joining us.

Thanks for joining us. This episode is available where you download podcasts, including SoundCloud, TuneIn radio, and Apple podcasts. It is also available on the SEI website at sei.cmu.edu/podcasts and the SEI's YouTube channel. This copyrighted work is made available through the Software Engineering Institute, a federally funded research and development center sponsored by the U.S. Department of Defense. For more information about the SEI and this work, please visit www.sei.cmu.edu. As always, if you have any questions, please don't hesitate to e-mail us at info@sei.cmu.edu. Thank you.