DoD Challenges and Potential Solutions

featuring Grace Lewis, Eliezer Kanal, Satya Venneti, Joseph D. Yankel as interviewed by Jeff Boleng.

Bill Thomas: 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 and operated by Carnegie Mellon University. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

In this series of podcasts, we are presenting excerpts from a recent SEI Virtual Event, *Is Software Spoiling Us?* Jeff Boleng, acting chief technical officer, moderated the discussion, which featured a panel of SEI researchers: Grace Lewis, Eliezer Kanal, Joseph Yankel, and Satya Venneti. In this segment, our panel discusses technical innovations that can be applied to the Department of Defense including improved situational awareness, human-machine interactions, artificial intelligence, machine learning, data, and continuous integration and deployments.

The panel also discusses barriers to implementing these technologies.

Jeff Boleng: I want to start talking about how some of those technologies can help DoD and government and maybe even why we haven't seen them helping as much. What are some of those barriers and things we can do about that? We are just free forming from here. We'll go through one more round of questions and sort of free-form some ideas on—what are some of those barriers and things we can do about that? How we might be able to better leverage these advances?

Grace Lewis: All the technologies that I talked about, I see them combined in improved situational awareness. I think that's something that the DoD could leverage—all these things together. If we talk about improved situational awareness using cloud computing, using the Internet of Things, using mobile computing, but on top of that we introduce this concept of edge computing, where you can imagine that you have these little clouds, baby clouds, whatever you want to call them.

The idea is that you push pieces of a cloud onto these computing nodes that are in proximity of mobile devices, of IoT devices. Then, now, you have brought the cloud to them. They have capabilities that they can use for improved situational awareness. They have data sets that they can use. They have platforms on which IoT devices and mobile devices can load data and that data gets sent to the cloud at some point for processing.

The idea is this continuum from cloud computing to edge computing to mobile computing to Internet of Things—that really improves situational awareness because you are bringing computing to the data, which is something that has been talked about before instead of bringing data to computing.

Some challenges that I understand are important challenges and real challenges for DoD is, one, security. That has always been a big challenge when it comes to cloud computing. When it comes to IoT devices, a big concern is untrusted supply chains. Because, IoT devices, everybody's building one now, right? There are tons of them, and I think the DoD should be able to leverage those.

Jeff: By and large, most IoT devices need to reach back to a cloud for some purposes, whether they are compute poor or whatever they are. So DoD doesn't typically like to give small sensors to people that continuously call home, right?

Grace: To address some of these concerns, a technology that is still emerging, but software-defined networking, software-defined security, being able to adapt security postures as things change in the network and the threat model. I think that technology should bring a little bit of relief to DoD, especially when it comes to improving situational awareness at the edge.

Another challenge that DoD deals with, especially at the edge, that my smart grocery list doesn't deal with, is operation in DIL environments: disconnected, intermittent, limited. Of course, if you want to have data flowing back and forth, it is not always possible, right? Technologies that we can leverage there are delay-tolerant networks. I know, Jeff, that's a topic that you like a lot.

Jeff: Named-data networking too. I'm bullish on named-data networking now.

Grace: That's right. I'll let you introduce that one. But delay-tolerant networking, to be able to deal with periods of poor connections. Intelligent data sharing where we know what to share, when to share and to whom. So we are not just spreading data all over the place. Intelligent routing, being able to use each other to be able to send data from point A to point B and being able to leverage data that is available at the network level to do that. Also, like I said before, if you are going to be able to push the cloud to the edge, you have to have ways to package those capabilities, whether it's data sets, whether it's some very intense, machine-learning algorithm, whatever it is.

But being able to package those and being able to imagine having a repository of containers, a repository of virtual machines that have these capabilities and being able to push them out to the edge, whether it's on demand, because *I'm at the edge and I need this capability*, or whether it's pre-provision. If you know you are going to be in a situation where you are not going to have connectivity, being able to go to a central repository and say, *I want to put this on my edge node and being able to take it out there*. So the ways in which I think the DoD could leverage a lot of the technologies that I talked about would be improve situational awareness, especially at the edge.

Jeff: Thanks. Actually talking about packaging the components in smart ways, Satya [Venneti] and I traveled to a NATO exercise in Romania this last summer. The translation engine for Google Translate on your phone, once you downloaded the language pack for Romanian, it operated without network connectivity. We were sort of out in the middle of nowhere anyway, but it was awesome. You can hold the phone up to any Romanian text and it would translate as best it could to English. We used it like crazy.

Grace: Right. You can imagine, the edge notes having all that information on there. Absolutely.

Jeff: Right. Yes. I've heard Cisco, I think, refer to that as fog computing. Everybody's got their own name, right? Cloudlets. Fog.

Grace: Yes. There's dew computing now.

Jeff: Is there dew computing?

Grace: There is dew computing.

Jeff: It's a little wetter than fog computing.

Grace: Exactly. In the end it's more or less the same. It's being able to be able to be closer to the edge.

Jeff: Yes, push the compute to the edge. Yes. I've read that the instrumentation on motor jet engines creates terabytes of data per flight hour.

Grace: Imagine that.

Jeff: You just can't move that data to the cloud or to the compute. You've got to move the compute to the data.

Jeff: OK, we are going to go to Satya then and talk again about the technologies that have enabled some of the civilian and commercial applications and how we might then start to use some of those in DoD or benefit from some of those in DoD.

SatyaVenneti: I think there is already lots of human-machine teaming going on in the DoD. On the left-hand side that is called Big Dog, and it's a robotic pack mule. On the right-hand side you have a loyal wingman. So it's a swarm of flying agents, which are autonomous, but there's an F-35 in the middle, which has just one human in it. It is already using a lot of human-machine teaming. What we really need is for humans to trust machines but also machines to trust humans, and that's how you build a rapport between humans and machines

So if machines should trust humans, machines should understand them, be able to predict what they are thinking. That is why we need machine emotional intelligence in the DoD. I think some of the factors that are actually coming in the way is, of course, the big moral issues and the ethics issues.

If the machine can collect all this data about me without my knowledge, how will that data be used, and am I always under surveillance? Bias sometimes creeps in. If you use machine learning and deep learning, sometimes it's a black box. You don't know what's going on.

Also, I think that the DoD needs to become more human centric in their approach and thinking. It has always been about the tech. Now we need to think about humans and how humans and machines interact together. We really need to bring in the human element. I think there is this thing called the Third Offset Strategy, where it talks about human-machine teaming and how we need machine emotional intelligence in the DoD.

Jeff: One of the main tenets, yeah. One of the major tenets of the DoD.

Satya: Exactly. It's like the one secret sauce. Like, it's, you know, our people, our secret, and nobody can steal them from us. It's important to actually recognize that humans are an important part of that equation and make humans and machines work together better.

Jeff: Yes. I heard one of the senior army leaders say at a conference that as we do pursue human machine teaming, if we replace humans with machines, that one plus one has to be greater than two, which sounds like a little buzz word. But really the point is we don't want one-for-one capability replacement where we take a soldier out of harm's way and put a machine there to team with somebody else. That combination needs to be far more capable, far more lethal, than the two soldiers were before that.

Satya: Exactly. I think humans and machines together can achieve greater things than just a human or just a machine because each of them sort of augments the other one and helps them.

Jeff: You have got that example about the chess playing.

Satya: Yes. So, you know, so this whole thing when Garry Kasparov, reigning chess champion, and this was 20 years ago, he was beaten by Deep Blue. It was actually like when actually people

started getting very worried about machines replacing humans. At that time what happened was people just had this big mistrust about machines. Then, eight years later, there was this whole new freestyle chess tournament that was arranged by Garry Kasparov where we could have teams of just humans or just machines or hybrids of humans and machines, and guess who won that tournament?

It wasn't a machine. It wasn't a human. It was a team of relatively weak humans and weak machines, but they had a really good process. That is really a very powerful result because it shows that the actual sum can be greater than each of the parts together. That is very important, I think, for us to understand. It's not actually machines replacing us. It's us working with machines to achieve greater things. I like to think about intelligence augmentation and not A.I., which is artificial intelligence. We actually use machines to augment our intelligence. That's how I like to think about that.

Jeff: Yes. I'm a terminal optimist.

Satya: Me too.

Jeff: I hate looking at the down-side. That's why the title for today's panel was, *Is Software Spoiling Us?* not *Why is Software so Terrible?* right? I too like the intelligence augmentation. I've already outsourced my memory to my cell phone. Well, my daughter gives me a hard time. She's like, *Dad, what's my cell phone number?* I'm like, *I don't know. I just click on your face, and then it calls you.*

Satya: I don't know how to spell anymore, because there's autocorrect all the time. I don't think that's a bad thing. I actually think it's a good thing because now I can think about bigger and better things. I can be more creative about other things.

Jeff: All right. Eli, we're going to jump to you. Same thing, so some of the enabling technologies. How might we better help, enable and empower DoD and the government to help benefit from some of those things?

Eliezer Kanal: A lot of what we've been saying earlier so far has already kind of touched a lot on the different A.I. [artificial intelligence] aspects. I mean just to highlight maybe one or two other ones. Image recognition, a lot of satellite imagery that's coming in. The DoD could definitely use some automatic understanding of what is in the image.

It's interesting because Google—I don't want to highlight Google too much. Many of the other players in this A.I. field have gone beyond simple image recognition, but that they can now identify that this [photo] is a smiling woman with a straw hat with her dog. There is contextual information. They could actually start extracting where she's sitting. There is a lot to be done

with images, so that is a very obvious relevance, I think, to the DoD. There are different areas that kind of tie back to what we were saying earlier about chess and Go and cars. There is a lot to be said about automated decision-making, and having an algorithm that can take in all the input situational awareness, as was being referred to before. If the algorithm knows everything, it's going to remember it a lot better. Sure, we can give it priorities, but it can definitely help with the decision-making process. There is an awful lot to be said for that.

The main problems that have stymied getting this all into the DoD. First of all, these all rely on huge troves of data. We have that at the DoD. In fact, they have far more data than they can handle, but the problem is it's frequently siloed and segmented, necessarily so. So, *this group can't see that data and this group can't see that data, because this data is highly sensitive, and we really have to be careful what it is that we want to put together*. There is a growing recognition everywhere, including in the government, that data is a liability. If I have data that means the bad guys can get that data. The only way to not let them get it is to not have it.

Jeff: Yes, but really, the flip side is the most true, right? Data is not a liability. Data is the lifeblood of modern corporations and modern capabilities. Actually cultivating and curating that data properly is this new immense discipline that we need to get better at.

Eliezer: Yes. It's simultaneously the fuel of all this magic, and it is the source of so many problems. Figuring out how to properly manage that is a risk balance that a lot of areas, including the government, are still trying to figure out.

In particular, if I have a certain amount of data, what's now being recognized. The government has always known—one example I am thinking of is one of the Tom Clancy novels—that some analyst figured out that there was an attack happening because he saw that there was an upsurge in the amount of pizza ordered.

Jeff: What do they call that? The Domino's Effect or something? Yes?

Eliezer: Yes. Exactly. So that's a very well-known example. But when you have a lot of data, there's a lot of small clues and the metadata leakage becomes very big. You were talking before about downloading the language pack to figure that out. Well, all of a sudden, if you're using Google's algorithm, Google knows that you just downloaded the language pack.

Jeff: Right. And they know where I am.

Eliezer: If you're on the cloud and you're not using it on your computer, they may actually know what you're interpreting. There are a lot of risks, and the government is still trying to figure out how to get past this. [To Grace Lewis] A lot of what you were saying about the fog and the edge, that's starting to solve that. It is finally starting to make its way into DoD systems.

Jeff: Yes, somebody at this conference a long time ago told me applications age like fish, and data ages like fine wine. Meaning that the data is the important thing to persist. Applications come and go. Analytics come and go.

Eliezer: Yes.

Jeff: But if we preserve that data.

Eliezer: Yes, interesting.

Jeff: Scott McNealy, the former CEO of Sun Microsystems, way back in late ’80s, early ’90s, he basically said, *Privacy is dead. Get over it.* I think the younger generation has a very different concept of privacy. I look at my daughters and the things that they are willing to Snapchat and Instagram about, yes.

Eliezer: There was a very interesting talk at a conference a year plus change ago where they showed that an Android phone with zero permissions—you have granted it the ability to do nothing—just by you walking around can figure out what city you’re in because it will map the path of your walking using the gyroscope to known maps of known cities and figure out where you are. No permissions whatsoever, and it can do locations. It has location tracking. It can find out where your house is, which stores you shop. It’s a scary amount of metadata leakage.

Jeff: Yes. So you just got to learn to ignore it. Just got to learn to be careful. Just hope for the best.

Eliezer: No privacy.

Jeff: Let’s just trust everybody again. No. All right. So Joe, let’s go to you. Same question on this round. The technologies that helped healthcare. You jumped in and actually really did highlight an area where modern software development practices really did help the government achieve capability more effectively than they could. Which, like you said, led to the formation of defense digital service and some of those other things that are going on now. Pull in on that thread a little more. What are some examples of how we might be able to better take those technologies to benefit the government and DoD?

Joseph Yankel: We just need to start to use them. We see our big successes. You have talked about Amazons and Googles. One thing they do well is they put out a new product, multiple times a day, right? It is pretty continuous integration. Continuous deployment. It is quite unbelievable. It is unique often to web presences, where you might have *I need 20 new updates*. But what happens is incredible. I have a developer somewhere committing code. I have enough automation in the system to know that my security is good. My code works. Everything’s been done, so I know this can go live.

Jeff: Massive amounts of automated tasks.

Joseph: Massive amounts.

Jeff: Which we really have ignored a lot in DoD and government.

Joseph: We ignore a lot of security. Security is mostly a concern after something bad happens.

Jeff: Right. It's a way to place blame.

Joe: We want to spend money once we've lost some big money.

Jeff: We want attribution, yes.

Joseph: What we want to do is we want to bring all the stakeholders in a project together. We want to change acquisition. We want to say, *If this is what we're trying to build, or this is the product we want. This is software, I need everyone here. I need some business folks. I need security professionals to talk about the implications at the beginning of my stages. I need testers to talk about what has to happen. I need the operations team. Operations, IT operations, and the operators often, which are the end users, to have some say in this process from the very beginning and to be included throughout the development.* This is just a new thought process for DoD, which has been relatively waterfall, relatively contract-based, which doesn't include… Let's think about it. We have three years to get a project done. I usually don't allocate a person from the government for three years.

He is going to receive this in three years and then take a look at it, and then say, *Wow. I can't get it to work. I don't know anything about this. Let me read about it. I'll get back to you in about six months, and I'll let you know what we think about this.* Well, that has got to stop. We need them to be involved early. I need to provide people and personnel in the beginning to receive this. One thing we want to push is early prototype. What I want is the HelloWorld version of an application delivered in a production-like environment very early. That way everyone has a chance to look at this, to talk about security implications, to talk about patching, to talk about supply chain. We can do threat modeling very early. We can catch things. We have a better chance of catching things. We have monitoring. You do all the things that you tack on later. In lieu of bad requirement gathering or old requirement gathering, this allows me to be iterative and change things. You often don't know what you want until you see it.

Jeff: Right. That is commonly true. The first release is never right on target. The other thing I find is if you iterate more often, you are taking your risk in smaller bites rather than multi-years of risk. Then, at the end of that, if you haven't achieved the goal, you can't scrap the system because you are hundreds of millions or billions of dollars into it, so now you got to figure out how to fix it.

Bill: Thank you for joining us. Links to resources mentioned in this podcast are available in our transcript.

The complete webinar, *Is Software Spoiling Us?*, is available in its entirety on the SEI's YouTube Channel.

This podcast is available on the SEI website at sei.cmu.edu/podcasts on Carnegie Mellon University's iTunes U site on the SEI's YouTube Channel. As always, if you have any questions, please don't hesitate to email us at info@sei.cmu.edu. Thank you.