The Future of Cyber: Security and Resilience

featuring Dr. Michael McQuade as Interviewed by Bobbie Stempfley

---

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.

Bobbie: Good afternoon. My name is Bobbie Stempfley. I am the director of the CERT Division at the Carnegie Mellon University Software Engineering Institute. My guest today is Dr. Michael McQuade, the vice president for research at Carngie Mellon University and a founding member of the Defense Innovation Board. The Defense Innovation Board is a federal committee that advices the Secretary of Defense on how best to advance technological innovation.

Welcome, Dr. McQuade.

Michael McQuade: It's very nice to be here. Michael, please.

Bobbie: Great. I found it to be really interesting this moment in time, and I thought it was a great opportunity for us to talk about security and resilience. For the past 30 years, we have really been focused on increasing security and resilience, and we keep not quite getting there. Most recently, I have been giving a lot of thought about the past and how that can be prologue for the future. I am really thrilled that you have been willing to come and talk to us today because I want to explore how those innovations that we are dealing with today at CMU and in the future can be so pivotal to help us with this secure future that we need. Before we get started though, I would really like to give you the chance to tell us a bit about your role here at Carnegie Mellon.

Michael: Great. Thank you. I am very happy to be here and have a chance to talk to people about cybersecurity but also about how technology innovation is changing the mission and the applications and frankly the implications of cybersecurity. So, my role at CMU, I tell people I have sort of three roles and depending on how you want to put the PowerPoint bullets together, maybe it's 3.5 roles. So, first of all...

Bobbie: Half a role.

Michael: Half a role, yes. First of all, the easy part is that with any research enterprise, the trains have to run. I have responsibility for the people who enable the research. So, the contract officers, the people who do regulatory compliance, the people who do technology transfer and monetization: all of the things that enable the brilliant people at CMU to do what they do for themselves, for the country, and for sponsors. So, that is one part of the job.

The second part, depending on how many ways you want to count it, is the yin and the yang of connections. So, part of the way I describe it is my job is to make sure that people who would benefit by knowing the brilliant people at CMU, know the brilliant people at CMU. And when I say CMU, I mean CMU, and I mean SEI, and I mean the whole ecosystem. So, we have people that are doing cutting-edge research. They are doing it because they are the best researchers in the world. There are people who should know about that.

The obvious case in point of CMU and artificial intelligence, if you look at the work that was done by the university over the last four or five years, to be sure people in Washington knew more about CMU, policymakers knew more about CMU. That is part of what I am doing for the university is to make sure people who know about us should know about us. The flip side of that is to make sure that the people at CMU know what challenges people out there have. Ultimately, it is a matchmaking job. So, to be able to be sure that a brilliant researcher in neurosciences is aware of the latest research being done in NIH [National Institute of Health], or that an application for AI that the Army thinks it needs for either a disaster recovery mission or for some other reason, knows about the people at CMU. So, those are the two connection parts.

Then the third part of the job is advocacy. Advocacy for the value of scientific research, the value of what universities and FFRDCs [federally funded research and development centers] do. And being involved in policy. Policy around how you balance open, free fundamental research with national security interests and making sure that that people who ultimately will make decisions that affect how we do and can do our job are aware of all sides of the issues. I spend a lot of time in Washington in that regard, and I spent a lot of time advocating for the missions that a research university needs to deliver.

The last thing I would say is maybe the soapbox I get on all the time. I am a profound supporter of what I think has been the most important collaboration in science, technology, innovation the world has ever seen, perhaps starting with World War II, maybe even a little before that. What the United States created in the last half of the last century and is in the middle of now is a collaboration between research universities, industries who understood the value of investing in the technologies for their future, and a federal government who realized its role in that, not just as a funder but also as a researcher, so the National Laboratory Systems, the FFRDCs. That triad, which was unique until recently in the world, has been directly responsible for the economy we have today and the world we live in for good or bad with what you think about the world we live

in. I think it is extraordinarily important for us to preserve that as a national asset and to also recognize that in this day and age, other countries have looked at us and they see how important that has been. So, we should not be surprised when they try and copy us.

Bobbie: So, I tell you, I could not ask for a better commentary about past being prologue. This whole idea of how we think about roles and responsibilities and capacity in this space, particularly in security and resilience, has been advantaged by that. But, also, to some extent, with the growth of industry in this space, we think that they have got all of the shiny, great next things. I really appreciate it. So, trains, connections, advocacy, and doing smart things in the future in the way that we have done in the past. I like it. That is a really great way to connect.

Let's take a moment if we can and talk about this idea of science foundations behind things. It is one of the things that in cyber in particular, we have a history of some science in good places, but then some, *We didn't know what to do, so we did the most logical thing we thought that may in fact not represent the best options.* What do you think about what has been the best innovation in this space that you feel is science-based?

Michael: I think there are a couple things I would bring to mind. Number one—and let me confound it with discussions about software in general, maybe the external person plugging SEI— all of the work that has been done in the community to make the process and the evaluation of software writ large to be a mathematical science, to convert that into a formal process and procedure. So, the work that has been done on design systems, the work that has been done on model-based methods; all of those are an attempt to turn chaos into a defined process because historically we have believed in our ability to add rigor to defined processes. I choose those words very carefully because at some point we start to talk about what is different now. I think at some point we have entered into a world where not only rigor matters, but probability matters too. We have emerged to a place where what got us to the dance may not be sufficient, and a much more probabilistic evaluation of threats and responses to threats, that is going to be necessary in the future. But, to your original question, I think this whole development of software as an engineering discipline as opposed to an art is directly translatable into the cyber landscape that we have now.

Bobbie: I think that is right. My background is mathematics and computer science. So, I see the world in a way that is definable by a language that is math and is programmable and changeable by a thing that is computing and computer science. This idea of metrics and measurement as the Holy Grail of cyber that we have never actually been able to accomplish, I think, comes because we have been so shortsighted about it. Your concept of probabilism is, I think, really impactful here. What can we observe, and how can we make good decisions about that? I think that is really very helpful. So, comment for me a bit then on, well, one, you are a physicist; where is my jetpack?

Michael: That is an engineering problem. That is not a physics problem.

Bobbie: Well, I think it is a little bit of both. What would you have thought we'd have solved by now?

Michael: I was thinking about this the other day. There are things that I am shocked at how far we have progressed versus anything I would have thought. As you know on the Defense Innovation Board we have been snarky and complaining about the poverty of the DoD in terms of capacity to compute and capacity of storage. But, in general, the availability of computation, bandwidth, and storage is light years beyond what I would have predicted 15 years ago, where we are now. I think the democratization of software as something people do is much further along than I ever thought. We could talk in a little bit about what some of the implications of that are. So, I think those are a couple of the biggest things.

What hasn't happened? Sort of the opposite question. Let me just say one other thing. So, I grew up in healthcare in diagnostic imaging. I would never have predicted the progress we have made in display quality and the ability to diagnose from soft media. First of all, the hoops we all jumped through 20 years ago to even move data around and present it to a radiologist, and a radiologist who was, God forbid, never going to do a diagnosis on a screen and never going to take cues from a cuing system. I am actually quite surprised at how rapidly that situation changed. I would argue, another theme we can come back to, this whole issue on the implications of dual use in driving technology and the security implications from it.

So, what has not changed or what has not progressed as fast as I thought? I would have thought we would have solved the assured identity and individual ownership of cybersecurity as a discipline long before now. I think we have made progress, but I think there is much more progress that needs to be made. I would have expected that…20 years ago I would have said we would have run out of Moore's law capability a long time ago on silicon standard CMOS [complementary metal–oxide–semiconductor] computer and memory. That would have forced us to have much-faster, alternate kinds of computation. I don't mean to downplay accelerators of one kind or another, but I would have expected us to be in a different place by now.

Bobbie: That is interesting. Maybe I am not capturing this right, but what I hear is some things forced us to make innovations in unusual places, right? Moore's Law. We innovated in some really unusual places. The other one—if I can pivot from your identity and individual security question a bit—that strikes me to be a real example of the nexus between technical solutions and innovations and adoption and policy activities as well, right? I think that ties us into this dual-use issue really interestingly. We seem to fight this all the time. We know what the right technical answer is. Is it really the best answer for this situation? Let's explore this idea of dual use here in the way you characterized it.

Michael: I come to this discussion both from a national security discussion and from what the department, for example, should be doing. And as you know we did this big software study around software acquisition. Historically, our national security position layered on top of brilliant people who do amazing things with dedication. You don't win wars by having an army that doesn't have soldiers who go out in the front and do so. Take that all as given, and the fact that I'm not going to focus on that doesn't downplay that, right? But we have also—and people use this term *offsets*—we have had major strategic overmatch capability. We could outspend out technology people on nuclear weapons. Under Bill Perry's leadership and a bunch of really smart people, we outspent and outengineered and out-invented people around stealth. Dual use changes the landscape because many of the technologies that are important for competitiveness in a modern environment directly depend on what the commercial sector also wants.

While it is very clear that the national security mission has exquisite imaging applications, it is also clear that many of the imaging technologies that are used for the commercial sector have direct application. The same thing on communications, the same thing on autonomy and robotics, all those sorts of things. The implications of that are two-fold. One, the places you will look for progress in the technology are different than, *I have people who do only that mission, right?* And so, the places you will look for expertise. The other implication is that you have to be very careful about thinking through restrictions you place on technologies. While it is very obvious that we don't want a lot of people running around with nuclear detonators, it is also easy to say there really isn't a commercial market for nuclear weapons. So, you are not going to hurt anybody by restricting nuclear detonators. That is a different story when you start to talk about restrictions on technology that are driving our economy.

People need to remember that all the things we talked about from a cybersecurity landscape relative to national security are just as important for the cybersecurity of our commercial sector. The damage to restrictions on the commercial sector, it's not a binary problem anymore.

Bobbie: The way you characterize dual use. My experience over the last several decades is thinking about what those two words mean together has evolved. Dual use used to mean offense-defense exclusively, and now it's...

Michael: It's commercial and national security.

Bobbie: Right. We bit the apple for COTS [commercial off-the-shelf], and we are all in. We have evolved to a place where not just critical infrastructure but just everything...

Michael: Lots of infrastructure, right? It also changes how you need to think about your investing. In an area of sensors for low-earth orbit satellites, there are presumably some exquisitely necessary sensors, but by and large, the department or the government probably

shouldn't be trying to out-invest the private sector, because the private sector has a driving need to have a business model that works. There is a win in there for us too. We just need to be careful how we capitalize.

The last point I would make is that the other implication of that is that technology is available to everybody. I think, in a lot of ways [we] need to recognize that in addition to places where we need to be unique, there are places where we just need to be faster than the other guy. Because we have just as much access—not even talking about illegal access to technologies—but they have just as much access to commercial technology as we do. We just better be quicker than anybody else at getting it into the place where we need it.

Bobbie: Speed is a really interesting dynamic. I know you have done a lot of work in speed in acquisition and speed in software. For me, I really struggle with understanding…with thinking about a future where the boundary between software and something other than software might exist. So, for me, this idea of how do we do things more agilely and faster, and how does that change how you think about the security and resilience concepts?

Michael: The first thing I would say is—and you are in some sense referencing also the software study we did—there is a very, very important first message in there. They always tell you when you try to make a point, you don't undercut yourself ahead of time, but the first point we made in that study was not all software is the same. My version of that when I was at United Technologies was, *You can make your own choice, but I am not going to ride on an airplane for which the engine-control software, which is the real-time software to manage it, has been crowdsourced. You can decide if you want to do that. I'm not going to*. That is a fundamentally different level of rigor than the software that we had people developing for an app on your phone to call the elevator. We do need to be very mature about not saying everything is the same and everything has the same restrictions associated with it.

The place where speed becomes really important is when we loop it into the validation and assurance of software. We need to be careful about which kinds of software—for which we do all the normal things that we can do to ensure the software is as good as it can be—but, we strongly benefit from a mentality that says, *Let me get it out there and see what happens and get rapid feedback on it*. Of course, you have to understand the consequences of that before you do that. If the consequences are low, and you are willing to take the risk of getting [it] wrong, and you know how to roll back and you know how to process, then a theory that says, *Speed matters more than a 100 percent accuracy* is a good theory, because I can continue to iterate on the loop. That is different than saying, *If I get this wrong, the banking system comes down*. I think that is the important part of the conversation that we always have to have, which is to scale ourselves to the risk.

Bobbie: We have any number of examples where someone thought their thing was less pivotal. Where they bought in on this idea that not all software is the same, but then they connected pieces that weren't all the same into an environment where they were treated the same. I think zero trust is an idea that is trying to help tackle that. How do you think about that, and how do you think about the things that you need to do to live in a zero-trust environment while you are also agile?

Michael: I would say two themes that come together. First is I would argue that when we talk about important disciplines for the future, *How many machine learning people are we going to need to make the country operate?* etc. The skills to understand consequences—what in the physical world we used to call Failure Modes and Effects Analysis—that skill is an underappreciated skill in software systems. Combine that with much stronger ability to do in-the-loop simulation of our software systems to be able to predict where systems could go. Of course, we never get it all, but, again, we go back to the sooner probabilistic view of things, but those are underappreciated skills in my mind. So, that's one thing I would say. What was the second question?

Bobbie: Zero trust.

Michael: Zero trust. Oh yes, OK.

Bobbie: You have been thinking things about this, I know.

Michael: I have been thinking about this. I think the concept of zero trust is something that we have put in one box, and we need to open the box up. We have talked about zero trust in some sense, purely as a networking issue. So, *How do I operate in a world where I can't assure the integrity, cybersecurity of the network, of the transmit*? The answer to that is encryption-at-rest, encryption-in-flight, etc. And, maybe it becomes encryption in compute. I think the concept of zero trust needs to be expanded much higher. It is, *What if I operate in a world where I can't trust anything*? *I can't trust my supply chain. I can't trust that the encrypted data is really the data that I thought it was*. There is a lot of work we have to do in the way we engineer systems to determine what level of trust we actually can have and what tools we have. So, there is a whole body of work going on—both here at the SEI and also up on the main campus and around the world on, *What does it mean to compute unencrypted data*? *What capability does that allow me to still have when I simply don't trust the network*?

My other example is—and I will be a little bit provocative here for a moment, *What is the likely path forward for 5G, right*? We as a country can decide that certain providers are simply not trustworthy. I think we no longer have the capacity to make those decisions for the world. So, we will be in a situation where untrustworthy hardware and software are out in the market. We need

to understand the limits of what we still will be able to do in a circumstance. Long ago, when people first started computing, the answer was or the statement was, *How do I make a reliable computer out of a million unreliable parts?* Go back to our very beginning, there is a lot of math, and there is a lot of formalism that has to be done on how can I do assured computing in an unassured environment.

Bobbie: We have never solved the problem of reducing the overhead of formulism. It is interesting that these are recursive issues that keep circling back around.

Michael: I would argue that we have solved the issue of overhead, but we don't have the solution because we have just required the system to do more. All of the overhead that would have been prohibitive 10 years ago would compute fast enough to take care of that...

Bobbie: Computing is cheap now. Storage is cheap.

Michael: Exactly, but we never sort of swallowed the benefit because we just move on to the, *Yes, but I need to do more. I need to do more*.

Bobbie: Yes, exactly. A number of really interesting thematics that we have talked about, this whole idea of, *How do we create an environment that is like the research enterprise that was built post-World War II that will enable us to have a technological foundation that is impactful and is world changing there?* is really key amongst us, this idea of probabilism and measurement being so important.

Michael: I think the other thing I would add into the overall conversation … so I will try to make some physics analogy here between what happens when the scale becomes statistical. I would argue that that is a major difference in the cyber environment today than 25 years ago. You know this, you have been through this a long time. First of all, we started with an assumption that everybody who was on the net, whenever it was, was a good guy. And taught us that that was not the case. Whether they are not a good guy because they are malicious, or whether they are not a good guy because they are not particularly smart or whatever. We got into situations where we needed to deal with that.

I think there are some pretty big changes that are happening now. One brought about by the democratization of software, just the sheer volume of how much stuff we need to look at and be assured is OK. If you project forward with what the Defense Innovation Board is trying to argue for, that is only going to get [to be] a bigger problem, because the more stuff that can be automated, the more stuff that's offered… and as my friend Milo always says, *An F-35 is really just a physical way to deliver software effects*. I mean that is the world we live in these days. So, I think that is one.

The second thing I would say is that I think we have reached a place where we have in some sense separated the person who desires an effect from the person who creates the effect. So, people use different words, *attack-as-a-service*. You can go on the Dark Web now and buy cybersecurity infiltration. So, you have a set of people who are not spending any of their time figuring out who and why to attack something. They are just spending all their time doing it, so you have a completely disconnected set of people. I am not sure that the same rules apply as to how you go about solving that problem in the world compared to the way we used to. So, scale matters.

Bobbie: That is interesting. I wish we had a ton more time on this one, because I didn't intentionally ask you here to agree with you, but I found that many of the things you brought up are things that we have thought about for quite a while. I think about a world where we are moving into robotics. CMU has been so impactful in the artificial intelligence space, not just the machine learning and neural network space, but artificial intelligence more broadly. It strikes me that I think about adversaries as attacking a very small number of things. One of the things that they target is our lack of understanding about how all the pieces come together and how the system will react, so our lack of ability to think about test cases and fault modes in impactful ways. We add the kind of speed and non-determinism that comes out of this robotic and AI-fueled world we are branching into. It really changes the way you have to think about security and resilience. I don't know if you have given any of that thought.

Michael: Yes, a little bit. I would just sort of maybe just to continue to riff on it. Let's sort of be blunt, the world we live in today, it is often the case that creating an effect is less damaging than creating uncertainty.

Bobbie: That is exactly right.

Michael: At the end of the day, we can decide what level of protection we want to make on our electoral systems, but people are going to go to election this year with a degree of uncertainty that what they actually do in that box or on that ballot is what gets registered somewhere. Just simply creating that level of lack of assurance, I think that is a new plan of attack. You don't even actually have to deliver the attack; you just have to deliver uncertainty as to whether the attack is going to occur. I think that is a very different place than we were before.

Bobbie: For me, that is a place where the security industry, and maybe to some extent the computer-science industry, has been insular and shortsighted. There are lots of lessons that you can learn from other domains that come in here that we don't need to learn ourselves. I have a former boss who called it the Christopher Columbus Rule: *always separate what is new from what is new to you*. We need to make sure that we are continuing to expand into this new space because there are so many pieces of it.

Michael: Yes. We have talked a lot about change over time. I think for a place like SEI, I think that is a relevant discussion because 30 years ago when the CERT mission was stood up, the people who cared about CERT were the people in Washington who said, *I need a CERT mission, because I need to protect national assets*. Fast forward 30 years, there are a lot of people for whom this is relevant. It goes back to what we said before, expertise is not all just in one place. There are portions of it which are highly specific to mission, but it is also a much broader collection of people who work the problem. As a society, we need to be sure that we are leveraging all of that together.

Bobbie: That is a really great place because it is in part about roles; it is in part about collaboration. So, back to the things that you started with: keep the trains running on time, somebody has got to understand how all this gets orchestrated together. Make connections you didn't know were made before. Advocate for all of the pieces and really think about that research enterprise that is necessary for what the next 30 years will be.

Michael: I think just sort of one code on the whole thing is, part of the growth of the tech sector has created folks that don't sit around waiting for someone else to solve the problem. A little bit of this is trust and confidence. A little bit is scope and scale. But, 25 years ago, or 30 years ago, if somebody said there was a cyber problem, people would have simply looked at the government to solve that problem. Nowadays if you are a large cloud provider, you are not sitting around waiting for someone to solve the problem. You own it, because it is your business model.

Bobbie: I think to some extent the question about what the government's role here is ties to a whole bunch of other areas, safety and security. I think it is pretty exciting. It is an interesting time because as a nation, we are really trying to project our own missions through and using this man-made domain. We have tied our economy to it in other sectors, so it is really, I think, an exciting time that we need to leverage.

Michael: It is an incredibly exciting time.

Bobbie: What do you like best about CMU?

Michael: I like the fact that if you do what I do, which is like proselytize for research, it is an incredible set of tools in the toolbox. I can find the most brilliant people to talk to anybody about stuff that really, really matters. So, that is number one. Number two, I have always tried in my entire professional career to never be satisfied or comfortable. One of the things I love the most about CMU is every day I find something that I didn't even think about before. It could be a crazy idea. It could be a brilliant idea. Sometimes it's both of those at the same time. But just the

ability for me to randomly run into people and say, *Tell me what you're working on*, and get blown away by it. That's the best part of CMU.

Bobbie: Oh, great. Thank you so much for coming and talking to me today. I really appreciate it.

Michael: It has been really good. Thank you.

Thanks for joining us. This episode is available where you download podcasts, including SoundCloud, Stitcher, TuneIn Radio, Google Podcasts, 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 US 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 email us at info@sei.cmu.edu. Thank you.