Improving Cybersecurity Through Cyber Intelligence

featuring Jared Ettinger as Interviewed by Will Hayes

Will Hayes: Welcome to the SEI Podcast Series, a production of Carnegie Mellon University's Software Engineering Institute. My name is Will Hayes. I am a principal engineer at the Software Engineering Institute. It is my privilege today to interview a colleague of mine from the Emerging Technology Center, Mr. Jared Ettinger. Jared, welcome.

Jared Ettinger: Hi, Will.

Will: Could you tell us a little bit about your background, where you come from?

Jared: Yes, sure. I have about 14 years of intelligence analysis and counter-intelligence analysis and operational support for the government. I worked in D.C. for a while. Earlier this year, in January, I moved up to Carnegie Mellon, Pittsburgh, and [I am] working at the Software Engineering Institute now.

Will: Great. So your field of work is in cyber intelligence in our Emerging Technology Center. And we want to make sure we differentiate cyber intelligence from cybersecurity, which is probably a term most people have heard a lot more of. Would you help with that?

Jared: So the way we here at the SEI at least to define cyber intelligence is *the acquisition of information to identify, track, or predict the cyber capabilities and actions of malicious actors to offer courses of action to decision makers to enhance or protect organizations*. The long and short of that is basically cyber intelligence is more like a subset of cybersecurity. It is going to be a force multiplier to your overall cybersecurity picture or platform for your organization.

It is something that you are looking internally in your network and outside in the world to figure out, *OK, what's going on in the world that I could use to provide some analysis and communicate that effectively to a decision maker that can enhance our cybersecurity for our entire organization?*

Will: I guess when most lay people think of cybersecurity, they think exclusively of how computers operate and firewalls and technical details. The way you have just described cyber intelligence, it really is many different modes of information gathering and processing.

Jared: Yes. You probably want to start off with *What are the needs or priorities for your organization?* Then, once you understand what those needs are, you are going to need to collect information to figure out, *OK, this is what I need to know. Now I need to go get that information.* That information comes from inside your network. Those logs—all that data that you are getting from your SIEM SYN, or DLP, or your IPS, or your IDS—and then going out into the world and figuring out, *OK, what else is going on? Whether there are geopolitical relationships. Whether you have business mergers or any type of situations going on with the supply chains out in the world or even cultures that your organization might operate in or have people as employees to figure out, OK, this makes sense. This is part of my analysis and how I want to communicate that to a decision maker.*

Will: The wide open nature of the field as you have described it seems really fitting for our Emerging Technology Center where we are really trying to be on the leading edge when things develop and find new applications and new uses for technology and methodologies that come about. Could you give examples of maybe a fusion that you have seen in your realm?

Jared: Some of the things that we are looking at at the Emerging Technology Center are advanced computing, applied analytics, and machine learning. Some of the things that we like to do with cyber intelligence is explore some of the newest and greatest technologies that are out there—whether it is machine learning, natural language processing, IoT [Internet of Things], even augmented reality and virtual reality—and try to figure out, *OK, does cyber intelligence have a place in that? Can those be a force multiplier for cyber intelligence and to help an organization with its entire cyber security platform? Those are things that we are exploring and are interested in and looking at right now.*

Will: Certainly being housed within Carnegie Mellon University, a lot of the fields you just mentioned are really frontiers that other staff at Carnegie Mellon are pursuing?

Jared: That is right. That is one of the great things about working here is that we have either the smartest person in the world working on some technology right now, or they know the smartest person in the world. We can tap into that and leverage that research and their creativity.

Will: I understand that a model of work and transition that you are pursuing and have had some great experience with is this formation of a consortium that you have been working with. Could you talk a little bit about that?

Jared: The consortium basically started, there is kind of a back story to it. About 2012, the Office of the Director of National Intelligence (ODNI) came to the SEI and said, *What is really going on in cyber intelligence out there in the world*? *Are there any best practices that we can learn here in the government*?

The ODNI came to us, and we did a study. That study is called the Cyber Intelligence Trade Craft Project, and that study basically went from 2012 to mid-2013 where we went out and met with a number of organizations, government, industry, and academia. We met with them and interviewed them and learned *what kind of cyber intelligence are they doing right now, what does their program look like, and what are the best practices and challenges they have?*

Then we wrote up a study for ODNI. That study included things like implementation, collection management strategies. How do you prioritize threats? How do you train your analysts? Here are some of the best practices, etc. in cyber intelligence. After that study was done, a number of those organizations that we met with said, *Hey, we really like this idea of collaboration and communicating with each other. Is there some form where we can continue this and keep this going?*

That basically started the consortium. That initiative and drive to do that started the consortium in June 2014 timeframe. That is how it started. What we do is we basically provide a forum, it is not not just sharing indicators of compromise. That is really not what it is about. It is a forum for sharing best practices and learning from each other and learning new technologies, what is going on in the world, and how they can apply that to their cyber intelligence program.

The other thing about the consortium is it is a venue to train. We provide workshops where people doing cutting-edge work in the field can come and lecture and teach members about what is going on in cyber intelligence, whether it is IOT, whether it is AR [augmented reality] or VR [virtual reality].

We also have these simulations that we run. That is one of the main things that we work on as part of the consortium, these simulations where it is a threat scenario where it can have a physical aspect to it but also a cyber aspect to it. Members send their analysts to get training, and then they have to diagnose or navigate through a very fast paced threat scenario and have to provide recommendations to management.

Will: It is kind of like a capture the flag but much more complex and diverse.

Jared: Yes, it is very complex. We make it complex on purpose to give it a real-world situation where they have a limited amount of timeframe to navigate through all the ambiguity that we give them, connect the dots and try to make some recommendation that will stop the threat from happening in the timeframe that they have.

Will: So they get experience hands on with tools and they get to hear about related scenarios.

Jared: Yes, so they are getting hands on experience with tools and also intelligence analysis, counter intelligence, and also being able to communicate effectively and to brainstorm and also think about how to go about approaching a problem, how to problem-solve.

One of the things that we do as part of our training is these human-centered design techniques where the participants get to think out loud and can communicate to each other in ways that they might not necessarily do on their own but through collective thinking and some affinity clustering or things like that or bulls eye diagrams. We can get the participants to think of some pretty creative ideas on how to navigate to that threat. But, it is also just not tools and analysis. Some of the softer skills, being able to communicate, being able to collaborate with other people on some of the toughest challenges when it comes to cyber.

Will: So you are doing more than helping people assimilate new techniques and new ways of doing things. You are helping them to train their approach and the human side of it in a way that you might not get from classes and books and such venues.

Jared: Yes, because you could be the greatest cyber intel analyst in the world, but if you are unable to communicate with your findings effectively to management, it really does not matter.

Will: And all of this in the context of where emerging technologies are being harnessed. You have a fairly diverse set of participants in this consortium—industry and government?

Jared: We do. It is government, industry and academia have joined in the past.

Will: Without naming any of them, could you speak a little bit about the differences in perspectives that those different kinds of organizations bring to the table?

Jared: I would say that they are all trying to figure out when it comes to specifically hiring. Who do you really hire? Do you hire the IT, very technical person that does not understand really or have that experience with intel analysis and how to critically think and connect dots? Or, do you hire the individual that is the intel analyst and train them on IT? Or do you hire just the generalist?

That is a problem space that really has not been solved yet, and I do not think there ever will be a solution because it kind of all depends on the organization and kind of what their needs are. But that is something that we have seen across government, industry and academia. They just do not know which. Is there a right answer? And quite frankly, there really is a…

Will: I have heard in different domains it is better to hire a people person and train them in the technology. Other domains, it is better to hire someone who is very well versed in the technology and help them get more effective at the people skills. This is an unsolved question at this point.

Jared: It kind of all depends on what you need for your organization. For me and my learning curve, it was the intel and the counter-intel and then try to get smart technically, and that has worked fairly well.

I think a good thing to have for any analyst getting into this field is at least a breadth of knowledge on a number of technical issues, and then have at least one or two verticals where you are really, really good at or at least you can say I can speak to someone in this field and kind of understand what they are saying, but when it comes to this particular area, I have a ton of vertical [knowledge], and I can talk to it.

Will: Putting people with various skills in those different verticals in the same room and having them do these simulations, there is some magic that occurs.

Jared: Yes. We try to generate that magic by putting people with different skill sets and different backgrounds together and make them work together. Also, what we try to do is purposely put information out there that would make them want to communicate with each other and whether that is true information, misleading information, something that will force them to get up from their chairs and talk to each other and say *Hey, are you seeing this? Does this make sense? Did you try this tool? What do you think about this*? And to have those discussions so that they can provide a decision maker with a comprehensive analysis when they come to that point.

Will: Having read some of the feedback you have received from past workshops, it seems like this is something you spent considerable time preparing for and depth and breadth of which you are covering in these workshops.

Jared: It is a long process to prepare for the simulations that we do. For the one that we just ran in August of this year, that process started in January. We came up with the storyline. We did it in collaboration with CERT also as part of the SEI. They are very helpful in running simulation, but the process really starts in January.

I can tell you that the first simulation we ran early days of the consortium, they basically had 50 intelligence reports that analysts had to sift through. For the second time we did the simulation, we had over 100. They are being flooded with reports that they are going to have to figure out and dissect in a very short period of time.

Will: So there is a time pressure?

Jared: Yes. There is a time pressure. So it is pretty cool. It is fun. It is exciting. It is one of my most enjoyable parts of the job.

Will: What other offerings beyond this do you have in the future?

Jared: I mentioned that we have the workshops where we bring some of the leading-edge people doing research and cyber intelligence. They can come and talk at these workshops, and the members also come and talk about *Hey, these are some of the challenges that we are having or some of the things that we have learned*, and they share and they collaborate that way.

One of the other things that we do here at the SEI is we build prototypes. If a member were to come to us and say *Hey, we really have this idea for a tool, but we just do not have the bandwidth to do it right now with the resources. Or, there is this new technology out there. We know it exists, but we can't have the resources in time to get to it. Can you help us with that?*

Part of the thing with the ETC, Emerging Technology Center, is that what we do is technology transition. So we will help them, build that prototype, and spend the time to get it to where they want and demonstrate that so they can be customizable for when we can deliver it to the member.

Will: This subject of tools is a perennial struggle for a federally funded research and development center. We often find ourselves having to tell our customers it would be inappropriate for us to endorse one tool or another.

It sounds like in the space you are working it is not even that simple that off the shelf tools may not serve the same kind of role in the technology area you are talking about contrasted with others. So this experience of using tools and building them together is a much richer part of your interaction.

Jared: We do not endorse any tool over another, but if a customer came to us and said *hey, we had this really good idea for a tool, is this something that you might be able to help us with*? So I can give you two examples.

One example was a member came to us and said, *hey we were interested in some way to better prioritize threats. Is this something that you can help us with*? So we were able to build something that could help them do that. Additionally, how do you select a vendor was the problem, and there's so many threat feeds that are coming in. There are so many vendors that are offering threat feeds. How does one organization select one vendor over another vendor? We helped not only build a framework for helping them to go through that decision tree but also a tool that could help them figure out *OK, I have this much money. This is what I need for my tool. This is the space that is out there. This is the timeframe in which I need it, and they can better select a tool that way.*

Will: I suspect in the context of a consortium where we have information being protected and people's concerns addressed carefully being able to share that conversation with more than one organization and have them learn from each other is probably a very powerful resource.

Jared: Yes, that is what the greatest thing about the consortium is, the ability of the members to collaborate and talk with each other. Again, it is not about sharing indicators of compromise. It is about saying *This is what works for us or these or some of the challenges we have. How have you guys addressed this problem?* The members drive the consortium. The consortium thrives by how much the members want to put into it. And they put a lot into it because they really do care about this problem.

Will: The way we staff our Emerging Technology Center has to be mindful of this. People with experience like yours really are needed to play this role, and you are not a person simply learned in a particular topic area as a university professor. You have more than that. You have kind of been there and seen real world situations. You have a number of colleagues who share that kind of experience. Can you talk a bit about the diversity of experience?

Jared: We have not only the members with a ton of experience but within the SEI and ETC, we have really technical folks. You have someone like me that has more of an intel, counter intelligence background. You have data scientists. You have individuals that are really smart when it comes to cybersecurity, people that are just strict researchers that are really good at researching things.

We have people that are experts when it comes to biometrics, when it comes to machine learning. We use all of their knowledge and brain power to try to help the consortium and bring whatever knowledge we can to help the consortium and their problems.

Will: There are other publications, webinars, podcasts that cover a great breadth of this experience, and I would encourage viewers to pursue that. Have you got a particular thing out on the SEI's website you would like to plug?

Jared: It is funny you mention that. We are going to be going around doing these information sessions to get the word out more about the consortium. We have an information session planned in DC. October 28 is the date. So if people can come, that would be great. Go to our website. On the SEI main page, you will see a link to it, and then you can register for that.

We are also tentatively planning to go to New York and Chicago [and Pittsburgh] as well to hold these information sessions. So far it looks like we have great turnout coming for the one in DC, so we expect hopefully can expect the same for New York and Chicago.

Will: In addition to the offerings we have talked about, are there educational opportunities people could pursue with you?

Jared: Yes. Actually, I teach an introduction to cyber intelligence class here as part of the Information Networking Institute at Carnegie Mellon University. It is a graduate-level course. In terms of the consortium, though, what we have been working on doing is getting consortium members access to particular slides of that course.

It is something that as we move forward with the consortium, we want to make sure that consortium members get some of that material because our goal with it really is training and education. If we can extend what I am teaching at the course in some variety to the members, then it is something that we want to do. At this point, it looks like consortium members will have access to certain slides as part of that class.

Will: Thanks very much for coming in.

Jared: It is my pleasure.

Will: This podcast is available on the SEI website at sei.cmu.edu/podcasts as well as Carnegie Mellon University's iTunes U site. As always, if you have any questions about this subject matter, please feel free to reach out to us at info@sei.cmu.edu. Thank you.