The State of the Practice of Cyber Intelligence

featuring Jay McAllister & Troy Townsend interviewed by Suzanne Miller

Suzanne Miller: Welcome to the SEI Podcast Series, a production of the Carnegie Mellon Software Engineering Institute. The SEI is a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You will find a transcript of today's podcast on the SEI website at sei.cmu.edu/podcasts. My name is Suzanne Miller, and today I'm very pleased to introduce you to Jay McAllister and Troy Townsend.

Jay focuses on cyber intelligence and educational outreach for the SEI Innovation Center. He researches and prototypes efforts aimed at developing and refining cyber intelligence methodologies, technologies, and processes to benefit the private and public sectors. Prior to joining the Innovation Center, Jay spent six years doing strategic, investigative, and operational counterintelligence and counterterrorism analysis for the Naval Criminal Investigative Service, fondly known as NCIS.

As a senior analyst with the SEI Innovation Center, Troy Townsend leads research and prototyping efforts aimed at improving cyber intelligence. His current work is focused on developing and refining cyber intelligence methodologies, technologies, and processes that will ultimately benefit network security. Prior to joining the SEI, Troy spent three years doing strategic, all-source, cyber-threat analysis for the Defense Intelligence Agency, including a year with U.S. Cyber Commands J-2 Intelligence Branch. Although separated from active duty, Troy continues to serve in the Air Force Reserve as a cyber operations officer, currently assigned to the Pentagon, where he supports the Homeland Defense Mission. In today's podcast, Jay and Troy will be talking about their recent research into the state of the practice of cyber intelligence. Jay, Troy, welcome. Thank you for joining us today.

Jay McAllister: Thank you.

Troy Townsend: Thank you.

Suzanne: To help orient our audience, why don't you start off by explaining the difference between cyber security, which we hear a lot about, and cyber intelligence.

Troy: That's actually a great first question, because it's the very question that we had to tackle ourselves, first. We were sponsored by the government to take a look at how cyber intelligence is being done in industry and in government. And, so that very first question of "What exactly is cyber intelligence?" is what came up first. So, we defined cyber intelligence as being the acquisition and analysis of information that is used to identify and track and predict cyber capabilities or intentions of people and enhance decision-making using that intelligence.

Suzanne: Why do you think that's becoming an important competency for the business community?

Jay: I think it's becoming really important because "cyber" transcends every aspect of business, whether you're doing human resources or business intelligence or physical security. Cyber plays a unique role in there, and the information you can take from all these different entities can formulate the posture that you need to have to keep yourself secure. A good example could be, in a cyber-security domain, you could identify a certain activity that's going to harm your network. Well, you could also then utilize physical security aspects of when, say, somebody's going to badge into a facility. If that's on a weekend, and then you start seeing weird network activity, well that's a correlation, and you've just done some intelligence work to figure out what is behind the method to the madness of these type of attacks you're faced with.

Suzanne: So, you're really synthesizing from a lot of different sources to get a better picture of what your security posture is, but also your business posture, right? Because cyber intelligence can be used to help analyze competitive threats as well as like security or other kinds of business threats, is that right?

Jay: Definitely, and especially in a time of resource constriction. Why should you worry about country X, if you have no plans, business-wise, to ever do business in that country. So, you can be smarter on how you allocate your resources. That's going back to Troy talking about the difference between cyber security and cyber intelligence. Cyber security is a lot more of that ones and zeros analysis. Well, "I found a threat. Why is that a threat to my network? Then, "Let's go ahead and fix that threat." Cyber intelligence brings in all the different aspects of the business to tell the story, which really then can help decision-makers who are not so technically savvy.

Suzanne: Excellent. So, you've been doing some recent research to understand what is the state of the practice of cyber intelligence in the business community and also to leverage knowledge about cyber intelligence from the government community. So where are you in that project, and sort of how did you go about doing this? I can imagine that this is a very sensitive area when you start asking people about, "What are your practices in cyber intelligence?" and they have problems in that area. So, how do you work that?

Troy: It's been sort of a challenge, but it's been really rewarding. We started out by trying to get a broad swath of industry to participate. So, we approached companies from multiple sectors: the financial sector, retail sector, transportation sector, education, non-profits, and state governments. We really cast a wide net. From that, we found that generally people that were more security-focused and didn't understand cyber intelligence were more hesitant to participate in this study.

So, a lot of respondents that choose to participate—and we ended up with 26 across government and industry—had some level of cyber intelligence already, some level of cyber intelligence capability.

Suzanne: A competency they had established.

Troy: ... already sort of established. A wide range in the maturity of that competency, but they at least recognized the importance of it. What was the rest of the question?

Suzanne: Well, just how you went about doing this, conducting this study so you could get this information.

Troy: So, we had the participants at that point, and we had to figure out what sort of a universal way of asking, "How you do cyber intelligence?" could be. The variance in participants went from an organization of one person, a one-person business, to a company that employed over two million people. So, we knew that there wasn't a one-size-fits-all cyber intelligence process. So, we created what we're calling "the cyber intelligence framework" and essentially we asked, "What are the key concepts that you have to be doing if you're doing cyber intelligence?" And from that we derived a set of questions to kind of dig into the details and see how well people are doing in those five areas. So, that allowed us to get sort of a standardized set of data to work with. We were able to bring that back and do some analysis on that data, and that created sort of a score card that kind of captured how people are doing cyber intelligence across the industry.

Suzanne: And, then you've aggregated that information so that people don't get all squirrely about having their names out in public about what they do...

Troy: Right, right.

Suzanne: So, what are the elements of the framework that you're using to characterize the state of the practice?

Troy: So, we came up with five core concepts: It starts with defining the environment. The environment is really knowing what your network is, what your user base is like, what those public-facing entry points into your network are, and then expanding it to look at the organization itself, right? So, "What's your market space? Who are your competitors? What data is important?" and "What's valuable to you?" right? And then also, "What are your potential threats? Who would want that data? Who would want to damage your company's reputation?" and sort of that whole omnipotent environmental look, right?

The next phase we're calling data gathering. So, based on how well you defined your environment, that dictates what data you really need to be on top of your intelligence activities. So, looking at internal network data, Firewall logs, or proxy-server logs, or host-based security system logs. That's one type of data that most organizations are able to get themselves, but then looking at sort of what's the enrichment data that provides context to what you're seeing on the network. What's going in the world? And, depending on how well you define your environment, you might be collecting too much data, which is just overwhelming for analysis, and so ...

Suzanne: And costs you money.

Troy: ... costing money and being ineffective at analysis. Or, you're missing sort of the key points. Maybe your net was too narrow. You're missing key indicators of potential threats that might be targeting you.

The next stage we're calling functional analysis, and that's really the technical analysis. That's the ones-and-zeros analysis, which many organizations are quite good at, and it supports the cyber-security mission. We suggest that that data can tell a bigger story. If you apply the context in strategic analysis, which is the fourth phase, that network data, that very functional data, combined with context from open-source data, sort of a—what do you call it ...

Suzanne: Multi-source kinds of data.

Troy: ... yeah, helps paint a bigger picture about maybe why somebody's going after that data. So, if you think of functional analysis as sort of answering the, "What's going on and how do I fix it?" type questions, the strategic answers the, "Who's doing this to me and why are they doing it?" type questions.

The last phase of the model is what we're calling reporting and feedback, and that's communicating the strategic importance of this network activity to the decision maker. A lot of times there's a challenge in getting technical data up to a decision maker in a way that they can understand that's meaningful to them. Strategic analysis helps do that by providing sort of the organizational context and the implications to the business and helps the decision maker understand the importance of investing resources in cyber security. So, you can see there's a lot of overlap between cyber intelligence and cyber security. The two feed off each other.

Suzanne: It sounds like a big part of this is really just enriching that context of where you're looking for data and how you're analyzing it and interpreting it.

Jay: I think so, and I think one of the things that we're finding is a really big, important aspect of this industry that needs to grow significantly is that strategic aspect. If you've been attending some of the bigger conferences, like Black Hat, the past couple years, all of a sudden this cyber intelligence term has become very, it's the new buzzword. So, people use it a lot, but when you go and ask them what they mean by that term, your answers vary widely. It is mostly a lot of cyber security-based information.

The interesting challenge we've had in dealing with participants—for some of them who have more of a sole cyber security focus—is explaining well, "Why does that 'who' and 'why' of the strategic aspect matter?" And, what we've found has really been interesting regarding return on investment. So, strategic can really help you go to your decision maker, and say, "This is why I need these resources." But, it's very tricky, because it's not like other areas of risk. Where another area of risk could go to the CEO and say, "Well, if you don't take these precautions, when you have an earthquake it's going to cost you this much money to repair the damage that will happen." It's a lot tougher to do in the cyber domain.

Suzanne: And, a lot of the damage is reputational damage for many parts of the industry, right? And, that is very difficult for people to put a price tag on.

Jay: That's a very key part that you bring up. It's explaining to these more cyber security-minded individuals who are doing amazing work, but they're not getting as much credit as they should because they need to go and state why it relates to brand. And you see that more and more.

Suzanne: It's all about trust. I mean we've seen cases where trust is eroded in one sector of industry or another and it takes a long time to rebuild that trust. So, nobody wants that trust to be eroded.

Jay: I think a lot of that, the trust issue, is at the heart of this project, because in a lot of instances, private companies don't trust the government. They don't trust other companies within their sector. They don't trust departments within their company, and it's getting over that. And you do that through kind of this information sharing and being willing to listen to the different opinions, but then seeing how each impacts the other.

Suzanne: So, you've had access to a lot of interesting information about practices and things that people are doing or not doing**.** Of the gaps that you've found in this initial study, which are the ones that worry you the most and why? Which ones make you not sleep well at night?

Jay: Well, the one that's kind of nearest and dearest for me, and then I'll let Troy finish up, is training and education. So, whether you're in the public or the private sector, there's nowhere you can go to say, "Give me a blessed cyber intelligence analyst." There's not that out there.

There’s not a specific career track or a continuing education track to build that analytical core and to build that skill.

We just finished a day-and-a-half workshop where we brought our participants together, which was really unique because a lot of workshops will be sector specific, but we had all of our participants across all of the sectors come in. One of the three challenge areas they were most interested in was this training and education, but they’re still trying to identify what are the most important skills.

Suzanne: What are the competencies that are needed. That’s a big challenge.

Troy: For me I think it’s that information-sharing challenge that Jay was talking about earlier. I think organizations in a lot of sectors haven’t realized that the cyber threat is a shared threat, that they’re not the only ones being targeted. Until they get over that—that notion that they can’t share that type of data, because it would indicate some sort of vulnerability or something—then it’s a real challenge to get everybody on board and collaborating on the same threat. And, also sharing government data with industry. The government has some cool capabilities, but the classification levels prohibit them being able to share with industry effectively. So, I think there’s a lot of room for improvement there as well.

Jay: I think another too is how do you deal with big data. One of the participants made an interesting comment, “Data is going to be the pollution issue for the next generation.” Forget about all the actual pollution out there in the oceans and the rivers and stuff. Data is going to be pollution.

Suzanne: It’s the intellectual pollution.

Jay: Yes, a great way to put it. Yes, the intellectual pollution, and so how do you deal with that. There’s amazing tools out there. There’s a multitude of tools. How do you filter through the noise? How do you identify and automate known threats and known data you see every day to parse that out to get to the unknown data. There could be a critical…

Suzanne: You want to get to the novel counterintuitive stuff, and get away from having the humans have to deal with the routine stuff. Is that right?

Jay: Right, because it can be a very labor-intensive process right now. So, how do we utilize the great minds at CMU or the Software Engineering Institute to start making solutions for that?

Suzanne: So, I think you guys are going to be busy for a while at least based on the few things you’ve said there. So, I have to believe that there are organizations listening today that are interested in proving their own cyber-intelligence practices. How can they learn from your research what steps they should be taking? How can they become involved in this if they would like to become engaged in this work?

Troy: In the short term, in the next month or so, we're going to publish publicly our findings that we shared with our participants this past week. The next step, from our sponsor agency, is to create what they're calling "an implementation framework." So, it's taking the best practices that we identified in our research and making them scalable, so that regardless of the size of the organization, you can leverage the best practices and start applying them where they need to be. So, that's our next major deliverable that we're hoping to get to by the end of the summer timeframe.

Suzanne: And, I'm assuming you'll need some test pilot participants, people that will try that framework out eventually. I know that there's a good bit of work before you get to that.

Troy: Right.

Suzanne: You should see Troy's face right now. He's got the scared look on his face, because he knows that there's a lot of work before we get there. Eventually that will be something that people will be able to participate in.

Troy: Yes, for sure.

Suzanne: Well, I think you've hit on sort of what's next for the work, and you've got plenty of it to stay busy with. I want to thank both Jay and Troy for joining us today. We look forward to seeing more results from this research. This is an example of kind of one of the best things the SEI has been able to do in the past of building communities around a problem like this and finding solutions that scale to different kinds of organizations, so I think that like I said, you're going to be busy.

For those of you who are listening, if you'd like more information about all of the SEI's recent research, you can download our technical reports and our technical notes at sei.cmu.edu/library/reportspapers.cfm. This podcast is available on the SEI website at sei.cmu.edu/podcasts and on Carnegie Mellon University's iTunesU site. As always, if you have any questions, please don't hesitate to email us info@sei.cmu.edu. Thanks very much.