Cybersecurity Canon Hall of Fame interview with Chase Cunningham on "Cyber Warfare – Truth, Tactics and Strategies." TRANSCRIPT

(SOUNDBITE OF RAMIN DJAWADI'S "GAME OF THRONES THEME")

Rick Howard: You're listening to the theme song of the HBO long-running hit "Game of Thrones," the unofficial anthem for the Cybersecurity Canon Project, a project designed to find the must-read books for all cybersecurity professionals because one of the greatest characters of all time, Tyrion Lannister, had this to say about reading books.

(SOUNDBITE OF TV SHOW, "GAME OF THRONES")

Kit Harington: (As Jon Snow) Why do you read so much?

Peter Dinklage: (As Tyrion Lannister) Well, my brother has a sword, and I have my mind, and a mind needs books like a sword needs a whetstone. That's why I read so much, Jon Snow.

Rick Howard: Which means it's Cybersecurity Canon Week here at the CyberWire, where we are interviewing all the Canon Hall of Fame inductee authors for the 2022 season. I'm Rick Howard, the chief security officer, chief analyst and senior fellow here at the CyberWire, and today's book is called "Cyber Warfare - Truth, Tactics, and Strategies" by Dr. Chase Cunningham. Enjoy.

(SOUNDBITE OF RAMIN DJAWADI'S "GAME OF THRONES THEME")

Rick Howard: I'm joined today by Dr. Chase Cunningham, the chief strategy officer for Ericom Software. Congratulations on your selection to the Cybersecurity Canon Hall of Fame, and thanks for coming on the show.

Chase Cunningham: Hey, thanks for having me. I was very pleasantly surprised to notice that somebody read my book, much less that it made it into a hall of fame.

Rick Howard: (Laughter) So more than your mom read it, so that's good to know. All right.

Chase Cunningham: Yeah, right.

Rick Howard: So you're no stranger to the Cybersecurity Canon project. Your graphic novels, "The Cynja: Volume 1" and "Code of the Cynja: Volume 2" were selected as candidates back in 2017 when they came out, and they are still great introductory books for children of all ages. But the ideas in this book, "Cyber Warfare - Truth, Tactics, and Strategies," published in 2020, is a much broader concept. So why did you write it?

Chase Cunningham: Well, I didn't think that there was a whole lot of nonfiction books that were very accurate on the strategic sort of side of cyberwarfare, and I also saw that there was a gap in folks looking at it from a real practitioner standpoint. There was a lot of kind of coverage mediawise and whatever, but I didn't find anything where someone who had done the work had written a book about it.

Rick Howard: And what brought you to that conclusion? I mean, you just thought there was a blank out there - that nobody was talking about strategy versus tactics? Is that the idea?

Chase Cunningham: Yeah. I found lots of books about kind of how-tos and technology and this thing and that thing, but I didn't see anywhere where it was really looking at - here's the big, broad strokes. And oh, by the way, here's how these new pieces of technology can fit into that for future engagements.

Rick Howard: Yeah. It's kind of my pet peeve in the industry, too. We like to focus on tactical things - the technical things, like how does this piece of malware work or how does this zero-day exploit work? And we tend to forget about, you know, what are we trying to actually do? What is the strategy that we're all using? You make a pretty strong case that the old perimeter defense model - something I call defense in depth - and we can talk if that's the same thing - if you meant the same thing - but that thing is designed to keep everything away from material data and material processes. And you say that's a failed concept because - lots of reasons, like allowing employees to bring your own device, VPNs, weak identity and access management programs, IoT management coming in to - you know, just general run-of-the-mill management. And I like to say that we scatter our material data and processes across multiple data islands - you know? - like personal devices, SaaS applications, cloud networks, traditional data centers. So did I get all that right, Chase? And if it's dead, what's the alternative?

Chase Cunningham: It's dying. I think we're continuing to age off of it. A lot of organizations are still in that old paradigm, and it's not - it's kind of the best of a poor choice, but we're moving away from that. Zero trust is becoming the thing that organizations are moving to because, strategically, it makes sense. I focus very

heavily on meeting the adversary at the door, I like to call it, and that's the approach I'm trying to take here - is you deal with the realities of the threat, and you counter where they're most likely to be, and that becomes your defensive posture.

Rick Howard: So you mentioned, like, strategically defending at the edge. Is that what we were talking about? You call it edge and entity security - EES. Is that what we're talking about here?

Chase Cunningham: Yeah. And that's - I think that's the follow-on evolution of moving past just strictly sort of human identity and access management. I think, really, what we're talking about there is everything nowadays has an identity - a router, a firewall, a thermostat, a user, a robot - you name it. We all have an identity, and it's going to operate on the edge of control. And it's going to be some sort of digital entity, so then apply your controls that way.

Rick Howard: So when I was reading through the book and you were describing EES, or edge and entity security, it sounded similar to the Gartner concept of SASE, or secure access service edge. Are those two things the same thing, or are they different?

Chase Cunningham: I think that they're in the same line and parallel. I think Gartner's approach is a little bit more limited because they're looking at the market specifics and which tools do what. For me, I was looking at the bigger, broad, long-term implications there. But I don't think that they're totally orthogonal to each other at all.

Rick Howard: So they're in the same ballpark. And so the SASE model says, we're going to flip the architecture on its head. You know, in the old days, like when I was growing up, the security folks would manage the security stack behind the perimeter - behind the dead perimeter defense thing you were talking about. But with SASE, and now edge and entity security, the architecture is flipping so that you hire a cloud provider to manage your security stack. And the first hop from all of your devices, wherever they are - you know, your employees' phones or, you know, laptops or cloud services, whatever they are - the first hop out to the internet goes through that cloud provider security stack, and then all you have to do is manage the policy. So how is that fundamentally different than this EES thing you're talking about?

Chase Cunningham: It's really not. I mean, I think that they're both in line. The interesting thing is the most difficult part of that problem you're talking about to manage actually becomes the policy. It's no longer that it's difficult to manage at

the entity level because the entities do what they do, and they need to access things that they need to access. But the control plane is the policy engine. And if you don't have a really good policy engine, you can't keep up. And like you were saying, because we operate at scale and because we operate so dynamically, you have to be able to do that with the automated solutions that have those capabilities.

Rick Howard: I realize the policy would be complicated, but it's one policy scattered across all those data islands we're talking about. So presumably it makes it simpler, but I understand what you're saying. It doesn't make it easy, I guess, is the way to say it. It's still going to be a complex policy, right?

Chase Cunningham: Yeah, it's got to be accurate I think is the most important part. The ease will come with rollout, but it has to be extremely accurate. And it's got to be something that's updated dynamically.

Rick Howard: One of the things you mention in the book is adopting, as a key and essential piece to this - is software-defined perimeter, which, by the way, is a horrible name. I know you didn't come up with it, but that's a horrible name to define a different way to do identity and access management. Can you tell everybody what that really means?

Chase Cunningham: Yeah. So what we're really talking about there is using policy engine controls combined with a piece of software, usually an agent, something like that, that will allow brokering of connections to individual things within the enterprise or outbound on the internet - doesn't really matter. But that's the difference in modern enterprise and modern business for where we are now instead of the 1996 technology, which was the VPN. You have control. You have granularity. You're tying things like user access and provisions on top of it, and you can get entities directly to where they need to go instead of just having access to the infrastructure writ large.

Rick Howard: You know, once I started reading about software-defined perimeter, it just - it's so obvious that it is ludicrous that you would actually try to go to the workload, this material workload, and try to log in there - and you know, and then that opens up all kinds of problems - instead of doing the software-defined perimeter where you go somewhere else. You log in there, and then that thing brokers the connection between you and whatever workload you're trying to access and nothing else. All right. You don't get carte blanche access to everything, just the workload you authorize to. So it makes total sense to me and...

Chase Cunningham: Yeah, it's becoming a pretty common practice. A lot of small and midsize businesses are still dealing with the legacy VPN legacy...

Rick Howard: Yep.

Chase Cunningham: ...Sort of architecture problem, and they'll migrate away from that as this becomes more commoditized and more easy to roll out. A lot of solutions in the market now that are specific to this particular need - and they get bigger, better, faster all the time. So it's becoming a very real thing in the space, which is good because it makes it more difficult for the adversary.

Rick Howard: So in the book, you discuss the origin of the APT term, advanced persistent threat, as a placeholder phrase for nation-states conducting a wide range of cyber operations from basic espionage to low-level cyber conflict. And then you list the major players that were - that existed in those environments in the early days, in the early 2000s, as Russia, China, North Korea and Israel. And then you make a point to say that 2010, with the Stuxnet attacks, with both the U.S. and Israel joining the fray, that kind of changed the game for everybody. And then Iran retaliating, and so we have the United States and Iran being top players. So is that the list - Russia, China, North Korea, Israel, U.S. and Iran? Are those the big top six?

Chase Cunningham: I would say those are probably still the big, major players. But the other piece that we know we all have to remember is - No. 1, the United States is an APT just like everybody else.

Rick Howard: Exactly.

Chase Cunningham: And then No. 2, there is no Geneva Convention in cyber that I'm aware of. So any organization anywhere that has that capability and connects to the internet is probably doing APT type of things. It's just really whether or not they get known for it.

Rick Howard: And so you make a point in the book to bring in influence operations, and you have lots of discussion about the technology that aids nation-states in doing this. What was the main point you're trying to make there?

Chase Cunningham: Well, I really saw that there was so much conversation going on around the elections and national security and whatever else. And to me, it was extremely clear this is the bridge between kinetic operations and espionage. And if you're able to influence things digitally at scale, you can influence things like the outcome of particular political events, etc. And that is where we've seen it, and

we're going to continue to see it - that the adversaries realize there's low-hanging fruit. So they're going to continue to target that application of control.

Rick Howard: So it's good stuff, Chase. And the book is excellent, so congratulations on that. This has been Dr. Chase Cunningham, the chief strategy officer of Ericom Software and the most recent author inductee into the Cybersecurity Canon Hall of Fame. Dr. Cunningham, congratulations, and thanks for coming on the show.

Chase Cunningham: Thank you so much. I really appreciate it.

(SOUNDBITE OF RAMIN DJAWADI'S "MAIN TITLE")

Rick Howard: For more information on the Cybersecurity Canon project, go to your favorite search engine and look up Cybersecurity Canon - that's canon with one N as in canon of literature, not two n's where you blow stuff up - and Ohio State University, the project's official sponsor.