Conference Debate Session II—Can AI Solve the Internet Cybersecurity Epidemic? Nobody Knows for Certain

Chair: Robert Kierstead

Special Agent in Charge, Seattle Field District, US Secret Service

Panellists:

Kumud Kalia	Chief Information Officer, Cylance
Slavik Markovich	Chief Executive Officer, Demisto
Greg Martin	CEO and Co-Founder, JASK

Robert Kierstead

Good morning. My name is Bob Kierstead. It's my pleasure to be here today at the Global Press and Analyst Summit, Silicon Valley. I'm the special agent in charge of the Seattle Field District of the US Secret Service. We operate in a transnational environment. We have an integrated protective and investigative mission. A large part of the latter revolves around the investigation of cybercrimes.

If anybody would like to contact me later, after the summit, please feel free. I have business cards also but feel free to email me, call me anytime.

Just briefly, I'll give you an overview of the Secret Service, show you where some of our cyber-asset locations are. We again are a transnational law enforcement agency so we have offices in the United States and abroad.

I'll just give you a brief case overview of our Roman Seleznev, a Track 2 investigation, which was one of our more prominent cyber-investigations. We'll enter into our debate and then after the 30-minute debate we will have a five-minute question-and-answer session.

The Secret Service's integrated mission is to protect the President, the Vice President, presidential candidates during election years, visiting heads of state. Recently in Seattle and the United States we've had visits of President Xi Jinping and Prime Minister Abe of China and Japan respectively, so we operate at a very operational tempo. We also are responsible for securing events, at national special security events such as State of the Union addresses, the inaugural parades, the United Nations General Assembly in New York every year.

Our investigations revolve around financial crime and theft of intellectual property. The Secret Service was actually established in 1865 as a law enforcement agency to combat the flow of counterfeit currency. In the US at that time, post-Civil War era, one third of the currency in the US was counterfeit. We were initially given the mandate to be a financial criminal investigative agency. In 1901 after the assassination of President McKinley we began protection of the Vice President and in later years the Vice President and presidential candidates.

We investigate counterfeit currency, credit card fraud, network intrusions and other types of data breaches. We also investigate, we find in the current - our current operational - our daily task is we deal with a lot of ATM skimming, ATM jackpotting and debit gas pump skimming. This is also - the Secret Service's mission is also consistent with the Department of Homeland Security mission to protect the American people in cyberspace.

This is just a snapshot of our cyber-locations. We have an electronic crimes special agent program, or ECSAP. We have a network intrusion program, and we also have a critical systems protection program which is part of our protective suite of services. So, when we conduct an advance for a VIP, for the President, the Vice President, we will actually go and look at HVAC, IT and other types of information technology assets in a site, and so we provide protection for not only the physical protection of those - of our protectees, as we call them, but we will also secure the IT space in which they operate.

Just a quick overview of our Roman Seleznev Track 2 case. Roman was a Russian national. He was a prolific credit card hacker. He would typically install malware on retailers such as pizza parlours and different types of restaurants and retailers, he'd exfiltrate that information, the Track 2 information off a credit card, he'd put it on a carding website and usually the US consumer, the US criminal or US criminal enterprises would purchase it. Roman actually had a testing service so you could see if the card was still vulnerable or not, and his crimes were responsible for actual losses of $170 million.

In the district for which I'm responsible, our first Track 2 or Roman Seleznev hack or manifestation of a hack took place in Coeur d'Alene, Idaho. We were called by a credit union to investigate what they believed was a hack into a Schlotzsky's Deli in Coeur d'Alene, Idaho. We imaged the back-of-the-house server so our unique signatures that we knew to be - that belong to Roman Seleznev.

A few months later we had a hack of a restaurant in Seattle, Broadway Grill, it was a very popular restaurant, received a lot of notoriety in the press in Seattle, and we ultimately in short order indicted Mr Seleznev. We had difficulty extraditing him from - or locating him in Russia. We tracked his movements abroad. We know he was very cagey or wary to travel to countries that did not have an extradition treaty with the US, he knew that we were looking for him. We know that from our post-arrest data searches.

In July 2014 we located Roman in the Maldives. We dispatched our agents to the Maldives, liaised with the Maldivian authorities; they agreed to expel him. This is Roman and his girlfriend moments before he was arrested. His first words were, “I thought the Maldives didn't have an extradition treaty with the US”. We took him into custody, put him on a plane, flew him to Guam for his initial appearance. He was there for three weeks. We ultimately had him transported to Seattle. He went through six sets of attorneys so the case took a while. Last year he was sentenced to - he was convicted in 2016 and last year he was sentenced to 27 years in Federal prison.

So, at any given time we're very busy and at any given time we are working on targets, whether they are in the US and abroad, and we have our methods and relationships with foreign law enforcement or our law enforcement partners abroad, the US Department of State and the Department of Justice Office of International Affairs.

Just an amusing side note. The picture on the left side of the screen was actually taken off Roman's laptop after we seized it. He fancied himself the Tony Soprano of the dark web, of the credit carding underworld, and he was actually revered by his associates as such and they presented him with a painting and its homage to the episode of *The Sopranos* where Tony's crew gives him a picture, a Napoleonesque picture.

Again, that's just a screenshot from the *Seattle Times*. Roman was very flashy with his purchases and the amount of money that he made, which again he made tens of millions of dollars through his illicit activities.

So, without further ado, I have the privilege to be the moderator of this very intriguing, fascinating panel discussion, *Can AI Solve the Internet Cybersecurity Epidemic? Nobody Knows for Certain.* I'd like to introduce my esteemed panellists. We have Greg Martin, Founder and CEO of JASK; Slavik Markovich, CEO of Demisto; and Kumud Kalia, Chief Security Officer of Cylance. I would like to give each of you a moment to make some introductory remarks. Greg.

Greg Martin

Thank you, and thanks for having me. I started my career as a hacker for the US Government, so finding myself as now an entrepreneur in Silicon Valley building technology including artificial intelligence, to help solve some of these problems has been a lifelong dream for me. So, having a lot of fun.

JASK is a 2.5-year old company. We are headquartered in San Francisco, California. We have just under 100 employees, and we build artificial intelligence for cybersecurity operation teams. The reason we founded the company is that there are not enough of us. We have a very, very large problem in the world. There are not enough skilled workers in cybersecurity and there are too many threats that the average organisation, whether it be the Federal Government or a bank or a local small credit union, has to deal with on a daily basis. I believe the latest numbers are over three million cybersecurity jobs that are unfilled, and this is in North America alone. The number is much, much larger as you look to the rest of the world.

So, if we do not develop artificial intelligence to start to accelerate identifying, automating, helping the analysts that we do have to deal with these cyberthreats, we're going to continually fall behind. We're going to have bigger breaches, more destructive breaches, and events like we saw here in the US with companies like Equifax which was simply a matter of not having the appropriate amount of resources to be able to keep up with the threats that they see. JASK were very proud to be on the leading edge using data science and machine learning to figure out how can we accelerate our cybersecurity workers and give them the ability to 10x what they do on a daily basis. So, thank you for having me.

Robert Kierstead

Thank you, Greg. Kumud.

Kumud Kalia

Yes, good morning. Thank you for inviting me here. A few words about Cylance. This summer, Cylance will be celebrating its sixth birthday. The company was founded with the intent of preventing malware with a mission of protecting all computing devices in the world. That's a very lofty mission. We're current at 16 million devices and counting. Over the last few months, you may have noticed that we passed the $100 million in revenues milestone, a very important milestone for our company. We're right now about at 850 employees and we are headquartered in Irvine in southern California.

My own background is I started with Cylance, I think this is now week seven so I know everything about Cylance, as the CIO. Previously, I'd been CIO in internet, energy, telecom and investment banking industries.

Robert Kierstead

Thank you, Kumud. Slavik.

Slavik Markovich

Good morning, everyone. Thanks for having me here. Like Greg said, I actually started in hacking but playing for a different team, actually, for the Israeli defence forces. I'm the CEO and Co-Founder of Demisto, and a few words about Demisto, I think. We are handling pretty much the same kind of problem that David mentioned when he had his keynote of how do you actually automate this whole abundance of security tools out there, how do you make sure that your analysts are trained and following a consistent process across those different security tools when they come to operate their security operation centre.

Like Greg mentioned, there is just too many of alerts, security tools and just too few analysts. I'm trying to think of - the only way of bridging the gap is trying to automate as much as possible of the workload and the process that those analysts have to go through, and they obviously are trying to make the analysis as efficient as possible, and I think we're going to talk about how AI can achieve some of that.

Robert Kierstead

Thank you, Slavik. For our first question, could you tell me about how you think artificial intelligence and machine learning can improve the security posture of a business?

Slavik Markovich

Great question. I think that when we talk about AI, everybody has a different concept of what it actually means. Here in the panel we actually have three almost different approaches to how to use AI for security posture and for improving the security of organisations. I think the big dream of AI or the big bet is it will solve all of our problems in security by just unsupervised learning, just throw all the stuff at it and it kind of manages all of it. I think we're pretty far from that yet.

The amount of resources that are required for that, the amount of storage, the amount of compute, is just not there yet, and so I think that we at Demisto really focus on what is the most low-hanging fruits that we can actually go after and help analysts be more productive. So, for a how-do-you-use AI, we actually look at things that are a bit different than anyone else in security, which is what are the actions and intents that analysts do in their day-to-day job that we can learn from and then we can feed it back to the same analysts when a new incident comes in.

So, we learn from the organisation practices in the real day - day in, day out, and we can try to do what we call - it's kind of an exploration into the sequences of actions that actually help solve an incident, and then the next time we encounter the same incident again, we can actually suggest that to the analyst and say hey, you know what, it worked in five different incidents before. That's one aspect of machine learning, and I think others actually use different types of low-hanging fruit to improve the security posture.

Robert Kierstead

Thank you.

Kumud Kalia

Yes. I think the approach we've taken at Cylance is to embed AI within our platform and within our solutions. Our aim is prevention and not response. I think in a traditional security implementation where there are multiple layers of technology tools, as you just heard from Slavik, the security analysts are often being overwhelmed by information from incidents and security events and log events, and it's hard for them to make sense of that. I think as long as there's going to be traditional security [stacks], there's a place for AI to try and make sense of that data that's overwhelming human beings, they're not able to process that amount of data.

But for those who are looking to move in a different direction then Cylance is really I think where the future is going to be where AI is at the heart of the solution so that you're not being overwhelmed by that amount of information, that the AI engine in the prevention tool is doing all that heavy lifting. So, it is preventing at source so that those events never get generated. That's really the essence of how Cylance is developing and serving our current customers.

Robert Kierstead

Thank you.

Greg Martin

I can tell you what AI is going to do for us now and what it won't do, and I think there's a lot of confusion in the space right now, so this is a really important topic. How we're using AI at JASK and how I see a lot of other Silicon Valley technology companies applying it is essentially to accelerate what we're already doing very manually with human workers, so taking those tasks that are repetitive that we do every day that are more scripted, we're giving those now to machines and allowing machines to do that work, because frankly, machines are better at some things like high-frequency pattern matching, if you're looking for these patterns over time in very large volumes.

Where a SOC analyst can get tired if they're working the overnight shift and they haven't had enough Red Bull, the machines can definitely crunch through that and find those patterns more quickly. What AI will not be able to do is take the human out of the loop. I believe that in our lifetime, most of us here anyway, that AI will not surpass the human ability to be the best defence against cyberattacks, at least the complex ones. I do believe that within the next five to 10 years AI will be able to deal with some of the more lower-level automated attacks, dealing with more financial crime, but the truly targeted government-grade attacker where there's a human behind the keyboard, the best defence for that will be a human behind the keyboard.

What AI will do, it will allow us to filter that advance attacker from all of the noise of the automated lower-level cybercrime attacks. This is where the industry is really struggling right now: how do I identify what I should care about versus the malware that I see every Monday? We had this phrase in cybersecurity we used to use years ago, that we're looking for the needle in the haystack, but really where we are today, we have a stack of needles, there's all these threats. The real task is finding what is that sharpest needle in the stack of needles that I have. So, the game has totally changed and that's what AI is going to help us with.

Robert Kierstead

Thank you, Greg. Kumud, we spoke earlier this morning about the increasing sophistication of cyberattacks. You brought up WannaCry and the Petya, NotPetya attacks and how we're seeing multiple attack vectors as opposed to single attack vectors now. How do you see artificial

intelligence and machine learning and how do we again continue to protect, guard and thwart cybercriminals who employ more sophisticated techniques?

Kumud Kalia

Yes. I think there was a lot of publicity around those attacks last year. Following the leaks of I guess tools, cyber tools that have been used privately by intelligence agencies being leaked into the public domain. Those tools being weaponised and put together in new combinations that hadn't been seen before resulted in those kinds of widespread attacks.

What people may be less aware of is that Cylance - the Cylance product, which had never seen these types of malware in the wild before, versions of our software that hadn't been updated in two years successfully detected and blocked these new software patterns. I think that's as profound a demonstration I can think of, of the efficacy of AI within cybersecurity, to say that look, our code had never seen these types of software, probably hadn't even been written in the combinations that were then released out for attack, and the software stopped these on machines. So, our customers that had that software didn't suffer these attacks.

Slavik Markovich

I think it's really interesting and I think the other side of the other players are actually using kind of the same mechanisms to try and evade a lot of those detections. I've seen people use evolutionary algorithms to evolve their malware and change it, and then test it immediately with all the prevention techniques and find the one strength in the evolution chain that basically bypasses the detection. When we say AI actually helps you with detection, you have to consider the other side as well, which is the attackers are also using the same mechanisms and tools to evade the detection. It's a game, an interesting game of cat-and-mouse as well.

Robert Kierstead

Slavik, do you think they're using it not only to evade detection, but are they also employing, or will they start to employ AI and ML against us?

Slavik Markovich

Of course, that's exactly it. Both in trying to evade detection, but also trying to find different ways to access the organisation and so on, definitely. You can actually do a lot of AI and A/B testing, seeing what works in a phishing email and you try 10 different versions across organisations and whatever works you can learn from it and continue, definitely.

Robert Kierstead

Thank you. Greg.

Greg Martin

Yes. I just want to be clear here that we are now in a full-on global cyberweapons arms race. WannaCry, this is not speculation, this tool was built from a stolen cyberweapon from the US Government, from the National Security Agency. That was weaponised and used against the public, public companies. This cyberweapon proliferation is the new normal, and we are absolutely certain that government entities are using AI to develop new cyberweapons.

We've seen this with things like WannaCry, which was based on a weapon called EternalBlue. It's about a five or six-year-old piece of technology, so you imagine what happens when the newer pieces of these technologies leak out, whether it comes from the US or another

government entity, the ramifications can be quite scary. Now with the open-source availability of some of these deep learning toolkits, really, any advanced actor whether it be government-backed military group or even an advanced actor working in the cybercriminal underworld has the same technology and capabilities that we do as start-ups in Silicon Valley and they are well funded, well organised, they are very smart and if we are automating defences, you'd better believe they're going to be automating attacks using AI.

Slavik Markovich

Definitely. It started even before that; you have to look at Stuxnet and all those strands where you can - even though the attribution is not necessarily there, you know that they were done by government and so it finds its way into other hands and being - [there's enough] commercial incentive to weaponise all of that.

Robert Kierstead

Thank you. The US Secret Service position is that prevention of cybercrime is paramount. We're also very attuned to the fact that if there is a - once it is reported on media that a particular company or corporation is breached, that's a damage to their reputation and that costs money, a lot of money. That being stated, when do you think is the best time for private sector companies to involve law enforcement in its cybercrime investigations?

Slavik Markovich

That's an interesting question. I think whenever there is a breach of public data, of someone, a citizen of the US, I think that you have to involve, and I think there are laws right now that can force you to involve the authorities in that.

Robert Kierstead

Thank you.

Kumud Kalia

I think most companies are aware of their obligations now for reporting and disclosure?

Robert Kierstead

Excuse me, I'm sorry.

[Inaudible]

Kumud Kalia

I think most companies are aware of their obligations for disclosure if they've been breached or hacked. Certainly, if certain sensitive information has been accessed they have a reporting obligation; it varies from state to state but mostly it's there. Then for law enforcement specifically, I think if there's criminal intent or criminal activity, then I think companies, whether they are obliged to report or not, would benefit from sharing what has happened and adding to the pool of knowledge as well as also maybe getting some assistance from law enforcement. In some case, you can honeypot the bad guys and then try and track their movements and predict subsequent behaviours or even then work with you and do like you did with Roman and try and pursue the perpetrators.

Robert Kierstead

Thank you.

Greg Martin

The private-public partnership has dramatically improved in the last five years, specifically due to some of the changes that were introduced during the Obama Administration. DHS has introduced ISACs and a new concept, ISAOs for information sharing. The challenge before would be that when you worked with law enforcement in US Government as a private company entity, it was always you would share the information out and you would never receive any information back.

That is what has changed in the last five years, so now the Government is taking a more proactive role. They're sharing cyberthreat intelligence on a daily basis, they're getting that to their trusted peers and they're accelerating the time to get that information pushed out, so we can incorporate those into our defences.

The situation and partnership has matured quite a bit and I think from a breach perspective it really helps organisations understand is this something I should care about, is this something that the Government has their eyes on or are tracking or is this just something that's run-of-the-mill malware. I think that partnership is entirely important, and it even needs to still mature more than we are today, but it's going in the right direction.

Robert Kierstead

Thank you, Greg. Questions? Sir?

Audience Q&A

Davey Winder, *The Times, SC Magazine*

Hi. It's Davey Winder from *The Times*, *SC Magazine*, and others. This is a question for Robert, actually. I'm interested to know how the Secret Service is using AI at the moment.

Robert Kierstead

The Secret service is technology agnostic. We're certainly interested in learning how we can be smarter faster in looking at technologies that will help us bring those that perpetrate these crimes and activities to justice. We're also very interested in knowing how this can complement our protective mission. Again, we have our critical systems protection program, so it does have a direct impact on how we perform our duties, so it is fascinating, and we are studying various AI technologies without committing to any particular one.

I'm sorry, do we have a question?

Kishore Jethanandani

I'm Kishore Jethanandani. I'm editor of *FuturistLens*. My question is about the new forms of cyberthreats, specifically using deception with adversarial learning or masquerading as trusted authorities once the adversary is inside the network, and generally leaving very little footprint. This seems to be a formidable problem which to my knowledge with existing paradigms is not solvable.

Slavik Markovich

Yes, cyber is hard. All-day low-and-slow attacks are very hard to detect and then a lot of them are detected almost by chance due to a mistake of the attacker that happens. But you are right, cyber is hard and you have a lot of noise coming from many, many different tools and finding that low-and-slow attack is definitely non-trivial, especially when [it sits] and uses existing credentials and slowly goes through your data. There are different ways of doing that. I think there's a lot of honeypot that you mentioned or deception technologies trying to lure the attacker to make a mistake, but there's no silver bullet, definitely.

Kumud Kalia

I think what we're seeing is maybe a little bit more sophistication, but the attack vectors are primarily the same ones that have been exploited for a long time. So, I think for companies that have their defences in good shape, they're not really susceptible to these attacks. Now, of course, the attack surface in a company just continues to expand and so it becomes ever more difficult to be that organised and disciplined to keep everything up to date and keep all the doors locked that should be.

It's relatively easy now for the bad guys to find out, even in companies that should be impregnable, to find the weak link in their armour. I think those are the things that then get exploited and not get noticed using low-and-slow kind of techniques. Sometimes, it's multiple exploits put together and so even if you detect one, you might not think to look in the other place. Sometimes, one attack will be used to overwhelm some resources to hide another stealthier attack underneath. So, I think those are just more sophisticated tactics that are being used by more intelligent attackers, but the techniques themselves are actually well known and documented and exploited for years.

Robert Kierstead

The gentleman in the front row. Sir.

Steve Cassidy

The man with a microphone again. Steve Cassidy - sorry, *PC Pro* magazine in the UK. I'm intrigued by the earlier comment that said that basically the NSA weaponisation of tools was just something we had to live, that it had become part of the landscape, because it seems to me that there must be a national cybersecurity picture of responsibilities and oversights and so on.

I'd be interested to hear from our speaker, more than from the panel, because we didn't do Q&A with you directly, right - interested to hear how your role fits in with the NSA. Are you ringing them up saying why are you guys letting these tools out, or is there actually no ability to do that and everybody is in their own silo and there's no responses?

Robert Kierstead

Are you directing the question to me? Okay. Obviously, we are primarily a law enforcement agency, not an intelligence agency. I don't know the best way to answer that question but it's - when we travel, if there's any information that's developed that's going to be a threat to one of our protectees, we would act upon it, directly to that organisation.

Greg Martin

I just want to add that cybersecurity is very hard and address the earlier question that was posed. The threat landscape is accelerating very fast because we have new attack vectors that didn't

exist before. If you hang out here for any period of time you're going to see cars driving themselves and they are connected to the internet and they are sending a bidirectional channel of information back to the mothership in the cloud.

We have companies that are now storing personal information and critical business assets in the public cloud, and that's a new thing and we're having to learn how to re-architect our cybersecurity defences to function in this new world. It continually grows and becomes more complicated, and this is why we believe that investing in technologies like machine learning that can detect low-and-slow attacks because they have no limitations on memory.

Humans can keep track of an attack that happened maybe 30 minutes ago or a couple of hours ago where machines can keep track of that over days and weeks and months. That's really where we're seeing a lot of uplift in machine learning technology and why it's being applied to some of these new growing threat landscapes like IoT, like self-driving cars, our personal devices. It's not a matter of it's just better, it's a matter of this is what we have to do as an industry to be able to keep up with the problem.

Robert Kierstead

Thank you. I believe that we are going to soon conclude so thank you very much. Again, thank you to all of our panellists, Greg, Kumud and Slavik, and I appreciate all your time the previous week, you really helped me make this really a lot of fun, so I appreciate it. If you have any questions of me again, please feel free to email me or see me; I'll be here the full two days. Thank you.

Manek Dubash

Okay, great.

Thanks again to the panel, and thank you Robert for coming along, and we'd like to see you and more people from your part of the world here in future. So, let's go for some coffee, but before we do, let me just briefly say that David Cheriton is available; if you've got questions for him, grab him, please feel free. Okay, let's go get some coffee and I think maybe bring it back in here when you've done, and we can crack on. Maybe we'll be on time, who knows? Thanks.

[end]