AVAR 2019

OSAKA-JAPAN

INTERVIEW

with Dr. Paul Vixie

22nd international cybersecurity conference organized by

ESET

ENJOY SAFER TECHNOLOGY™

Interview with **Dr. Paul Vixie**

ESET security evangelist Tony Anscombe sat down with Internet pioneer *and Farsight Security* CEO Dr. Paul Vixie, who co-invented some of the services that are central to the internet's fabric, to discuss a range of issues that affect the global internet today. Here's the transcript of the entire interview.

Tony **Anscombe**

Dr. Paul **Vixie**

I'm sitting here with Dr. Paul Vixie, who's an internet pioneer, and currently the chairman, CEO and co-founder of Farsight Security Inc. Dr. Vixie was inducted into the Internet Hall of Fame in 2014 for his significant contributions to work related to the Domain Name System (DNS) since 1989. This includes the invention of many of the monitoring and filtering capabilities now used by nearly all DNS services and anti-spam technologies. Hello Dr. Vixie!

Hello!

So, Dr. Vixie, you're presenting at AVAR later this year. Now, AVAR has been taking place for some 20 years, along the way marking, in a fashion, the internet's evolution. What's on your mind ahead of delivering the keynote at this year's AVAR?

Well, of course, current events always dominates our thinking, so it's difficult to remember how we got here if your hair is on fire right now, so what's got the world's hair on fire at the moment is the war for control over the DNS resolution path, which has been going on for about 25 years, and it's getting to be kind of a hot war. It used to be a cold war. I've been to Japan many times, of course, my degree is from Keio University, but this will be my first time speaking at AVAR, and I am honored to do so. I think what is on my mind is letting people know that there are some internet plumbing issues that are about to have a big effect on enterprise security as a practice.

Right, okay, that's a jolly interesting use of plumbing. What do you think: a big blockage is on its way?

I wouldn't say a big blockage, I would say that things are about to go the wrong direction down some of the pipes.

And there's something we don't want to happen! So, given the growth in the Asia-Pacific area, how do you see the evolution of the internet in that region?

Well, there's a coincidence happening, because the internet started out, of course, as a science and engineering network, and in the 90s it began to commercialize, privatize, and now, as we speak here in 2019, it has become the backbone of the world economy. Almost all economic values and cultural values are transmitted through the internet and held in internet accessible places somehow. That has coincided with a really dramatic rise in the Asia-Pacific region, to where they used to be the makers of the world, and the rest of the world were the consumers, but it's now starting to become a very unified world, and Asia is a huge part of the global economy, both as a consumer and as a producer. You can see that in the standard of living that's increased, you can see that in the population that's increased. You can see that a lot of our technology is not just manufactured, but also created in the Asia-Pacific region. So, with both of these huge growth events coinciding, I believe that the next phase of the internet's growth is going to have a more dramatic effect in the Asia-Pacific region than it will on the rest of the world, as the Asia-Pacific region is on a growth trend where it's ready to absorb whatever industries and technologies the internet can help it with.

Yeah, they've probably not had some of that legacy either; the internet started more in the West, so they've kind of had that leapfrog effect.

They really have, fiber in the home was a big deal in Korea and Japan even 10, 15 years ago, and we still don't have it commonly in the US. In the US, there are a lot of households that are still fed with DSL over copper. They didn't have to do that in Asia, because they didn't have DSL, so there was simply no reason to ever have that stage; they went straight to the good stuff.

Yes, I still have copper at home, I kind of enjoy that circle thing when I'm streaming video! Yeah, I thought that was actually part of the program! So, this year's theme at AVAR is hacker vs counter-hacker, from retribution to attribution: what role does DNS, or better DNSSEC, have to play in this most serious of games? Do you think researchers, developers and educators generally pay enough respect to the fact that DNS underpins so much of the function of the internet, and more importantly internet security?

I think that recently, the last few years, a lot of people from the rest of our tech industry have begun to understand the importance of DNS, and that has caused a lot of companies to come into existence hoping to leverage certain parts of DNS as a way to make their business plan work. And a lot of good innovation comes out of that type of disruption, but what that means for us, attending a conference like AVAR, is that pretty much everybody has to catch up now. It's no longer okay that only some of your competitors and some of your attackers understand how DNS works and how important it is. We all, in order to defend our networks, have to understand how DNS is used, and how it is served, and how we are deploying it. And DNSSEC is kind of a special problem because it's not pretty, it's not a very architecturally beautiful protocol, but it can be made to work, it does work, and when it is made to work, it is able to create trust relationships over protocols like HTTPS or TLS much more quickly and without quite the lengthy supply chain of learning whether you should be trusting your counterparty. But DNSSEC has taken so long to standardize and deploy that some parts of the digital economy have decided not to wait and are moving and just assume DNSSEC is dead – it's not. So, the web people are now inventing their own way to do what DNSSEC was originally crafted to do, and I don't necessarily blame them for their impatience. It's been two decades, after all, but the fact is they're wrong. The internet is much bigger than the web, and we have something, DNSSEC, that will work for all of it, and we all have to unite behind that. But again, that decision is going to be made in every company that owns a network, and that means that every company that owns a network is going to have to educate themselves about these issues.

Yeah, I mean, if you take a standard enterprise company, do you think some of the attacks against DNS infrastructure have helped bring it to the awareness of a board level in enterprise companies where DNS would have probably been an IT acronym they would never have heard of?

That sort of thing never lasts. So certainly, when Dyn was attacked a couple of years ago, that woke a lot of folks up. Gee, if Twitter and Microsoft – various large companies – were all affected by attacks against this company I've never heard of, I probably want to learn more about that. And it ended well for the Dyn people, because having been brought to the world's attention, they got an attractive buy-out offer from Oracle, but I would say that the rest of the world probably had some new thing to worry about that they didn't know enough about the following week. So, it's not a sustainable rise in awareness, and that's what we have to do.

Okay, so a new, a more collaborative approach to cyber security seems to be afoot, I'll give you an example, I'm from ESET and we contribute to the MITRE ATT&CK framework, and also we've provided IOC detections from EDR solutions and domain name system protection services, to build use cases and get feedback on products and data. Do the wider shifts favoring a collaborative approach to cybersecurity strike you as a boon for the security industry?

Yes and no, probably more no. So, I'll remind you that ESET has been doing this a lot longer than the MITRE ATT&CK framework has existed, and so when the current fad in information sharing, threat sharing, intelligence sharing was STIX and TAXII, ESET was involved in setting those standards and abiding by them and their products, and benefitting from them. When it used to be IODEF and IMDEF, before STIX and TAXII, once again ESET was right there. So, I think that the companies that have been in this for the long run are always ready to explore the benefits of cooperation and figuring out how to trust maybe your director competitor, if it's going to be of benefit to the customers of both. And so, I wouldn't want to call this a new trend, what I would want to say is that, now that it's an industry, we're seeing a lot of investment get dumped into it on the condition that, 'This company can only succeed if it learns how to share'. And that means that it won't be just a few long-range vision companies that are trying to do the right thing, it will be everybody for a while, until there's a new fad.

Yeah, an interesting point comes from what you've just said: we all compete, in the security industry a lot of us compete with each other, but at the end of the day the people that work in all these companies have a common goal, and that's actually to provide the protection of the systems, and a safer internet, a safer environment for communications to happen. So I think that's a really valuable point just to highlight.

I think that if you and I are both running security companies, and I have the goal that my customers are going to be a lot more secure than yours, therefore I'm not going to cooperate – I will fail, because my customers will never be a lot more secure than yours, because there's a certain averaging effect. If your customers are getting successfully attacked, they're probably in the supply chain for my customers, so we have to work together at some level.

Yes, absolutely, and I think that's one of the things I value within the security industry is the collaboration across the board. So you've co-founded SIE Europe, an organization that aims to secure the digital economy via the collection, aggregation and sharing of data, without personally identifiable information. However, profiting from data, which until data protection regulations with teeth and low-cost high-return gambit, has become a wide-spread business model. How can *SIE Europe* and other parties protect the wider digital economy while in some way undermining the gold rush taking place around data collection that is with the tens of billions of dollars, certainly in the US.

Well, a certain number of early adopters of the gold rush always profit. Famously, pets.com was founded at the end of a gold rush period, and is the last time that anybody was willing to put money into a company that sounded like it had no possibility of success, because it, in fact, did not succeed. But, up until the week before you could put money into anything and you'd do well as long as you got out before it crashed. I think we have to watch for that because it's a repeating pattern in history. Now, my own contribution here is that I started the first anti-spam companies called MAPS, the Mail Abuse Prevention System, back in the mid-90s, and we were very dedicated to making the world a better place. We invented the first distributed reputation platforms, called the Realtime Blackhole...

...List, or the RBL, which is still in use; everyone who sees this video is receiving email that has been filtered by at least one RBL system, and they will for the rest of their lives, and their children likely also. However, we didn't solve the problem, in fact we lost badly, and we got sued out of existence. That caused me to wonder about this gold rush mentality; what is it about how we're trying to solve this problem that makes it so difficult to do the right thing, and in the end, my conclusion is that we had chosen the wrong strategy. We, at MAPS, built walls, the spammers built roads, and road-builders always beat wall-builders in the long run, so what SIE Europe is designed to do is all about building roads. If somebody wants to compete with us and somehow monetize what we are not monetizing, they're going to have to build roads to compete. I've got to say that if we've got people competing to build better roads, we're going to get a better world no matter who wins.

Yes, I love that analogy, the walls and roads, that's a very visual way of thinking about it. Yeah, spam continues to be an interesting issue. I think I actually receive more spam than I do good email in my personal inbox these days, but maybe that's just because I've subscribed to too many things. Now, with stronger hints at both government and business seeking to carve up the World Wide Web into regional internets, firewalled environments etc., how far have we stepped away from a free and global internet? As for the perceived trade-offs, restrictions for better, more perceived security: are there other ways forward?

I've been fighting against the outcome of gated communities and walled gardens. I really did not want the internet experiment to end in a whole bunch of armed camps where pretty much you can't go anywhere unless you've been pre-approved and put on some list of people who are allowed to visit certain parts of the internet economy. Here, in the US, we have a long tradition of girl scouts and boy scouts going door to door and selling cookies to their neighbors, and that teaches them a lot about what retail sales can be, and how to talk to people, and how to use your voice. So, it's been a good thing, and I would hate to have it be that the internet version of that can no longer happen because: now, if you imagine a girl scout trying to get into a gated community to sell cookies there, the guard would probably say 'No, you can't come in, little girl'. I don't want that; none of us who helped build the early parts of the internet would like to see it end in that way. On the other hand, I think that we do have to do something; the internet will...

...not change the way cultures develop. I know that a lot of folks believe that if they can just make the internet strong enough, it will overcome authoritarianism, and it will cause individual freedom to come to everybody; that's not realistic. These authoritarian regimes are here for a reason, and they have a lot of resources, and they'll spend whatever it takes to make sure that their culture is not nominated by the internet's culture. So, I think we have to take a different approach. My idea here is if we could get all of the nation state actors to agree on certain norms, like you won't interfere with elections in other countries using social networking or something along those lines, and we could back that up with well-enforced treaties, so that if you do that kind of thing then you will be a pariah, you will have no container ships landing at your ports anymore until you stop acting that way, then we might be able to find a common core of the internet experience, where at least as far as that much then we all agree. We've got this for nuclear proliferation, we've got this for child abuse, or sexual child abuse, we've got this for human trafficking - we do have norms in place between countries who would otherwise be at war with each other about other reasons, but they can all agree on certain things, and I think there are some things about the internet that need to reach that level. Otherwise, it's going to be a destabilizing influence, and we're going to end up with some spectacularly bad outcomes.

Yes, well I think there's two sides to that isn't there? There's the nation-state piece and the much bigger picture, but I'm going to get back to your analogy of the girl scout selling her cookies. The danger is of course, the internet is a monetization pit for cybercriminals and people wishing to make money in the wrong way. Unfortunately, they're dressing as the girl scout and selling their cookies, which have unfortunately gone past their expiry date, they're not good cookies. I think it's a big challenge, of how you validate somebody's identity on the internet going forward to make sure that it's the right person that you're dealing with.

Identity has been changed -- not just the way we think about identity, but also the way we experience identity in our lives because of the internet. So, I'll point you to eBay, an online auction site. You almost always can't find the real-life identity of the person that you're buying from, it's a fairly anonymous experience. Obviously, the company knows, and obviously the seller, the buyer, can reveal themselves if they choose, but they don't need to it. What they have is a reputation within the eBay system, so, although you...

...don't know necessarily what their credit rating is, and you can't find out 'Are they in good standing with their bank?' There's a lot of traditional methods we would use to validate that this seller, this buyer is somebody you want to do business with. We don't have that, what we do have instead is: 'What is their rating on eBay? How many times have they done well? How many times have they done poorly? How many others reviewed this pseudonymous identity?' And this is working -- we're not seeing an awful lot of illegal materials being traded on eBay. It's one of the few examples I can think of where the online version was not less safe than the pre-online version of something. And I think we're going to have trouble because of that, deciding that you must reveal your identity before you can do business. I think that we're going to see a new middle ground between fully anonymous and fully known, where people will be able to do their work, or their business, or their communications on the internet without necessarily having permission that extends all the way to their fingerprints. I know that some countries don't want it to work that way, and they'll certainly be holding out. But if a bunch of other countries can figure something out that works, and is a middle ground, then the countries that hold out will eventually fold, and come back and say 'Alright, we're willing to live that way'.

Yes, it's interesting, maybe there's some type of solution there that your identity is never transmitted, but trusted.

Indeed. We have some systems like that, PGP is an older example, Blockchain is a newer example, where someone can take somebody else's word for you being a trustworthy person without necessarily knowing who you are. So, you can build chains of trust that don't also convey identity.

Yeah, so DNS, security, filtering, there are a lot of points of intersection around how users may leverage the World Wide Web in the future. Amongst the points that you would like to drive forward at AVAR, is there any homework you'd like to see researchers and AVAR's attendees do to prepare for your discussion?

Well, I hate to assign homework, but since you've asked, I'll say that probably the biggest driving force in most of our controversies raging today is that people don't know the history of DNS. They don't know how it works, they don't understand what their choices are, they're just doing what everybody else does. We have a generation gap between those of us who remember a time when every network had to run its own DNS servers, and then we have the newcomers who have never seen a DNS server, they have just always used Google's 8.8.8.8 or whatever. And I think it is important that the people making that choice be aware that they're making a choice, and they have other choices, and what the issues are. I wrote an article, *The Benefits of Locality in DNS Resolution*, that is a quick ten-minute read that explores these issues and explains again what choices you have, and what are the implications of those choices, so that we don't have people just blindly deciding to send their DNS outside their company, outside their house when they don't need to. And there are some hazards if they do.

So, for the attendees of AVAR, Dr. Vixie did just set you homework, so I'm sure he'll be marking your attendance and whether you've diligently done your homework! So how do you see the increasing push of recursive domain name servers, RDNS, away from customer networks and towards ISPs and then over the internet affecting concerns over loss of privacy? Has this very process been a key driver into pushing us into the current situation with GDPR and CCPO?

I think so, I think that any trend which has been official to anybody will accelerate unless it's opposed. In this case, the people who've been running name servers, a lot of ISPs for example, have been running name servers and they can see all of your traffic. As a result, they understand what questions you're asking, they see what answers you're getting, and they might do any number of really questionable things. They might sell key words related to your identity to advertising: 'Hey, this guy's doing the following...

...things, I know because I can see his DNS requests'. That would be an example of abuse of position. They might also look at some of the questions you're setting and see that maybe you had a typographical error, you transposed two letters in a domain name that you're looking up, they might decide that instead of sending you the DNS error message that will tell you 'Hey that doesn't exist', they will give you some alternative answer that goes to some advertising provider that they have a deal with. This is an abuse of position, and, if you abuse your position, you will create opposition, and that's what's happened. We wouldn't see this kind of counter-action through things like GDPR if there weren't a reason for it. It has to be motivated before it can happen. So, there is a way to sort of split the middle here. Some early internet memes say: if you're not paying for the product, you probably are the product. What that means is that if somebody out there on the internet wants to give you something for free, they probably have some motive. I'm not saying that it's a terrible motive and that they're out to get you, I'm just saying that their reason for doing it is not to make your life better, they've got some other reason and that reason may be compatible with your life being better, or it may not be compatible. It may be that what they want for themselves may be bad for you. So, what I advise people is not only think for a long time before you outsource a critical function like DNS, but don't use any critical system without a contract. If you can use it without having to first get into a contractual agreement with the far end, it's probably bad for you.

Yes, yeah, I like your discussion there of: If you're not paying for something, then you're probably the product. It's something I've told my son for many years, especially when you're downloading apps on phones, because sometimes it's not always obvious how the app vendor is actually being paid. Do you see a time where, with this growth of privacy legislation coming across many places in the world, do you see a time where actually consumers will understand what their data is valued at? And maybe see how to trade their data in that way?

I think, sadly, that I have to say no, most people just want to live their lives in peace and go about their business and not have to be an expert on everything they touch. Most people want to drive their car without knowing how to build one, and so on. There's very much a limit on how many things people can have expertise in, and, as a result, they count on their...

...governments to take care of the rest. I think it's a bridge too far to imagine that the average consumer will understand the data economy well enough to participate in it on their own behalf. They are counting on regulators, legislators, police to protect them from attacks that are bigger than them, and that they cannot all, as a whole population, comprehend. It is very much like we count on our national militaries to defend us against certain threats that are out of scope for us as individuals, and that's what this really is. I like GDPR as a model, because it says that our digital output, the little digital breadcrumbs we leave behind us everywhere, belong to us, and anyone who wishes to use them has to get our consent first, and they have to get that consent on a use-case by use-case basis. Under GDPR, just because you have someone's personal information you are not allowed to use it any way you want, or, if you have permission to use it in one way, it doesn't automatically give you the right to use it in some other way. While I think there's going to be a lot of fine-tuning, GDPR is definitely a move in the right direction, and I would like to see the rest of the world emulate this practice.

Yeah, I think a lot of the world is, you have CCPA coming here in California, you have legislation in Chile coming, you've got legislation in Australia, and Canada have got their anti-spam laws and data-protection laws, so I think the world is moving that way. It'll be interesting to see where that ends up, and hopefully from a personal perspective, I'd like to see global legislation. Maybe I'm being far too optimistic, but wouldn't it be great if my identity was protected everywhere in the world? But, I'm truly the optimist on this.

I think we will not live long enough to see a global government that could have global legislation. When it comes, it could be good or bad, but, again, I'll harken back to some treaties; it may be that in order to trade container ships, you have to first reach agreement on things like human trafficking, and that, if we can add to the list of things you must have agreement on, then certain norms about privacy would be on that list.

Yeah, absolutely, because the world is becoming a far smaller place - we're all becoming much easier, mobile, to move around. So, what is driving the new web-based DNS over HTTPS or DOH protocol now being strongly pushed by Mozilla and others? Is this a project that will actually increase and stabilize privacy?

Well, it doesn't add privacy, which is my first concern with it, because a lot of the people who are pushing the DNS over HTTPS protocol have made what is basically an outlandish claim that it gives you more privacy – it doesn't. There was a protocol created about a year earlier than DNS over HTTP called DNS over TLS. DNS over TLS has the same privacy -- you don't get more privacy from DNS over HTTP than you already have from DNS over TLS. There's no privacy gain here, what you're gaining is somehow the political effect that your network operator will not be able to see your DNS transactions -- by not seeing them, they won't know that they are DNS transactions, which means that every user, every application, every IoT light bulb, everything can now decide for itself how it wants to satisfy its DNS needs. And I can tell you as a network operator working in the defense industry my whole life, I need to see what my users and applications and devices are doing in DNS in order to know which one of them is an intruder, which one of them is malware, which one of them is part of a Botnet, which one of them is a poisoned supply chain. Let's say it was a bad motherboard BIOS update, and all of a sudden the motherboard is making bad DNS queries that the user knows nothing about. I have to be able to see that in order to keep my network secure, and so anybody who comes along with a project like DNS over HTTP that says 'Yeah, we want to make it impossible for the network operator to interfere with DNS operations', they don't understand my life at all. And they're trying to make, I guess, life easier for a dissident in some authoritarian country, but they're not, because if you are a dissident in an authoritarian country where the ISP is controlled by the government and you use DNS over HTTP because you think it will make you safe, make you able to criticize the government even though that's illegal, you're going to jail. Using DNS over HTTP will not keep you out of jail. There is no benefit to a dissident by using this protocol, and, at the same time, the cost that DNS over HTTPS places on family parental controls and corporate security controls is so much greater than any benefit that has been proposed, that I cannot understand the DoH people's heads are at.

Wow, that was an education for me, Dr. Vixie, so thank you. So how can we better protect the log of Stub DNS transactions where personal information is present in the future, to ensure privacy for all users of the internet? Is privacy the strongest weapon that security practitioners have in their pockets?

So, privacy is not an absolute, rather privacy is relativistic. For example, privacy at home: if there's a new internet protocol that makes it possible for the Cloudflare company to have its own private relationship with my underage children through the DNS over HTTPS protocol which deliberately bypasses parental controls, then I feel like that's a little bit creepy, and Cloudflare should not want that. And I don't think that my underage children have a right to privacy when they are online, or a right to privacy versus their parents' oversight. Once they become adults and move away, then yes, they're free of me, but until that time I'm responsible for their safety so I am going to find out what they are being offered and who they're talking to, and that's my responsibility as a parent. I'm not ready to have Mozilla and Cloudflare tell me that 'No, those days are gone, your role as a parent no longer includes that, we, the big tech industry are going to take care of that for you'. So I think the way that we are going to be keeping these transactions a little bit more private – where privacy means: is seen by everyone who should see them, isn't seen by anyone who isn't in that first set – is that we're going to run local DNS servers as we did in the early decades of the internet, and there's never been a day that it wasn't the right thing to do. It's gone out of style because of inertia, because it's very sexy when you put 1.1.1.1 on a T-shirt, everybody sees that and they want to type it in. So I understand that the dark side is quicker, easier, more seductive, but I want to tell you that there are costs to taking the easy way out, and I'm involved right now in a big project to try to get DNS to be encrypted everywhere, but to have it still available as a control point for cybersecurity inside of family networks and inside of corporate networks. I think we can get there.

Yeah, I hope so, I think looking at it from a slightly different perspective, it's the abuse of those look-ups that are unencrypted. We're back on those people that are monetizing that data, somehow we need to combat their misuse of data, to allow the correct use of data.

Yes, but I'm not sure that doing that with technology is going to be an end-point. I think that'll just be part of a gradual escalation, and so I'll tell a story about a company called Comcast. They're a big ISP here in the U.S., and they were caught red-handed, I've seen the PCAPs that prove it, where they were sending TCP reset packets to end-points that they thought were involved in internet file-sharing. This was basically an anti-piracy effort. People were illegally sharing copies of music and movies and whatnot, and Comcast wanted no part of that, so they were injecting false traffic into their network to break certain communications among their users. And they got caught. It was a big scandal, ten, twelve years ago, and a lot of people said 'No ISP should be able to behave that way, we need laws, we need regulations, we need protections', and, to their credit, Comcast eventually said 'Yeah, you know, that was the wrong thing to do, we shouldn't have done it, we're not going to do it again'. And I am pretty happy with that outcome, because if they do it again, they'll get caught again. I've got a certain amount of assurance that they are fulfilling their promise to us by not doing that because, if they did, I'd see it, or somebody would see it and it would be news, it would get out there. And so, I'm a Comcast customer at home and I actually trust their name server, which is 75.75.75.75. Everybody wants to use the same number four times, and they had one so they did it. And, you know, I'm a DNS aficionado, it is a hobby, it is in some ways my life's work, so I have tickled that server from a number of different directions that maybe normal people wouldn't and I can tell you it's fine. So, if you're a Comcast customer and you've got somebody telling you that you shouldn't trust your ISP's DNS server they're lying to you. That's old information, you can trust Comcast. Now, I can't speak for other ISPs, because I haven't been a customer of them all, I haven't tested them all myself, but we are working, a number of us have been in this industry for a while, are working on trying to come up with a way to qualify the quality of your local ISP and their DNS. So that if they are respecting your privacy, and they are not interfering with your work, and they're just giving you a good DNS server that is closer to your house or business than anybody who is further away, then you should use them. If you find yourself using an ISP that does not qualify, you may want to change ISPs or use a VPN. . Those are both better approaches: changing ISPs, running your own name server, using a VPN, all of those are better than depending on a non-contracted party at the far-end of the internet from you, whose legal environment is that country not your country. That makes no sense, there is no economic or engineering sense to be had from using a DNS server that is further away.

No, well the good part of what you just said is that I am also a Comcast customer, so I'm feeling a lot better now being a Comcast customer, because maybe I didn't trust them before you just said that, but however their customer support...well, we won't talk about that. So, Dr. Vixie, I'd like to thank you for spending some time with me today, it's been fascinating, I'd like to wish you good luck with your presentation, your keynote at AVAR.

I'm really looking forward to it, thank you for coming out and doing this interview.

Thank you.