**Paul Vlissidis**

Spoiler Alert. Some of the ideas, actually, that some of the fugitives have had to sort of stay below the radar, have been quite impressive. Two of the fugitives that won the show, were using canal footpaths as a way of getting around the country, which was actually a stroke of genius because there's almost no CCTV on those kinds of things. And so, they were just off the radar and that was a stroke of genius really.

**Ajay Bains**

Welcome to the Demystifying Cyber podcast by Lancashire Cyber Foundry. I'm your host, Ajay Baines. I currently work as a Business Support Officer for the Lancashire Cyber Foundry. We're passionate about helping businesses realise their digital potential. We work with eligible organisations across Lancashire to support them by placing cyber innovation at the heart of their strategy. Today we welcome a special guest, Paul Vlissidis, Paul is the current technical director for NCC Group, which is a global cyber and software resilience business. He's the author of “How to Survive the Internet”, and has also featured on Channel 4's critically acclaimed Hunted series, where Paul has taken up the role of Head of Cyber. Hi, Paul, welcome and thanks again for agreeing to kickstart our podcast series. To start with, it always kind of helps to set the scene. So can you tell us a little bit about how you kind of initially started out in the world of cyber and how your career has unfolded.

**PV**

Yeah, sure. I've been in the industry for a long time now and in fact it wasn't even called the Cyber Security industry when I started in it. So that shows you how long I've been in the in the game. I actually started out as a programmer. I did a computer science degree and started out as a programmer in industrial systems, moved into kind of safety systems and the risk around safety systems. And then saw the opportunity to get involved in security, which was quite new at that time and around about the mid-90s and then sort of took it from there. Really, I consider myself quite lucky because at that time, you could get into the industry essentially as a hobbyist. Effectively, you didn't need any formal security qualification or any of those kind of accreditations in order to get started. So from that point of view, it was an easy start for me, but it was an exciting time, still is, to be fair, has been all the way through.

**AB**

Yeah. Now, so it's always good to kind of see how those who are amidst cyber how their kind of career unfolded and how they initially kind of entered it. One of the things that I wanted to kind of touch upon was your book “How to Survive the Internet”, so I've been reading this in the kind of lead up to speaking with you today, always kind of helps in terms of context. But for our listeners who may not have read this Paul covers areas such as how to reduce your digital footprint, how to protect yourself when out and about, and what to do if you are a victim of an attack? One observation that I made that I think is quite interesting. Was the simplicity of language that was used to make the book kind of down to earth and readable. I wanted to drill down a little into where you kind of decided to take this simplistic and non-technical approach and what your thoughts are on the kind of traditional language that's currently being used in cyber and also what the likely implications of this are.

**PV**

OK. So that that's a really… I mean well, first of all, thanks for reading the book. I really appreciate it. But yeah, the decision to use non-technical language was extremely considered in the sense that what it occurs to me is that one of the downsides of our industry in my opinion is we are literally up to our eyes in jargon everywhere you turn. It's more jargon, more acronyms, to the extent that you can often be in the room with people who are using jargon and you know that not everybody in the room knows what all the jargon means, right? So, if I and I think it's a curse rather than a blessing, I understand the need for speaking in precise terms when you're dealing with technical topics. So, I can still respect the need for some jargon and some technical terminology. But it occurred when I wrote the book, I was aiming it at a wider audience of non-technical people who are exposed to risk on the Internet as we all are but don't want to be put off by lots of technical terminology and lots of jargon. So, and it was actually quite a challenge for me because I'm a technical myself. I come from a technical background so I, as I say, you know our first kind of urge really is to use the correct technical language when we're talking about the thing, the problem with that though, is often the person you're talking to doesn't really have all of the background and the context and the technical understanding to be able to sort of get what you're saying. So, you have to sort of kind of dial it down and so that was one of the reasons the book actually was quite painful to write in many ways.

I kept having to do that. And I had a brilliant editor, actually who was a non, I deliberately picked a non-technical editor, and she was fantastically supportive because she would keep coming back and saying no, I still don't understand what that means. So, I would keep dialling it down and dialling it down and hopefully I've succeeded. I don't know. It's one of those. My sister-in-law is extremely non-technical and she found the book too difficult, so I haven't quite hit the mark. But then you know, maybe it was a first attempt. Let's put it that way.

**AB**

No, it's really interesting and I look forward to kind of to finishing it. But I guess kind of given that we're on the topic of kind of the language that's currently being used. I know that a few articles and stuff that you've done before, you've referred to kind of the language being used as being kind of quite militaristic and masculine. But I guess this kind of leads us on to the topic of diversity and how we can make cyber more diverse. I know the National Cyber Security Centre released a statistic more recently, which was I think that women make up just 16% of the UK Cyber Workforce. I know there's a lot of work being undertaken to change this and one example of that was more recently here at Lancaster. We hosted an event in collaboration with Cyber Girls First, we're doing some fantastic work across the country, so we had a group of kind of around 70 schoolgirls that attended our campus and they were able to take a tour and we were able to kind of shed light on the opportunities that exist within the cyber arena and we had some fantastic female business owners who attended and they spoke to the girls about their experiences of working within the digital sector. Whilst this work is great, there's always more that can be done and so I wanted to kind of ask you about, you know, your thoughts on how we can make cyber more diverse.

**PV**

So, when we talk about diversity, I mean I like to think of it in its widest possible sense. So, I also want to make it more accessible. To, you know, we talk about neurodiversity now. As well as all of the other sorts and I think that's really important because it is a fascinating career. It involves. So many different aspects you know, historically we tend to think of it as kind of geeky sort of technical hacker type people. But actually it is now much, much more than that, because there's a very strong people component to security as I think we all understand. And we have not as an industry been very good at engaging with that, we tended to stay in our technical box and I think, OK, the last few years things have changed. But I think that's also opened up enormous opportunities for we need a lot more different talents to come into the industry and to help us to sort of come up with solutions that are going to help people to solve these problems and mitigate these risks that they face, I also think that even within that technical sort of environment, it has been quite a male dominated environment historically. I don't think that's a shock for me to say that you know. And I think that. And yet a lot of problem solving and the creative problem solving that takes place in there is often better suited to people with a more kind of creative mindset than in some technical people have. And I don't want to denigrate anybody here because I think that it literally takes all sorts to make these problems solvable. And so, yeah, I just think that there's so much more we can do. I honestly think the secret though is to get in as early as we can within the education journey. To try to engage people with the sort of career opportunities in cyber from a very early age. So. And I'm talking even down as low as primary school age. You know, I think that the earlier it we can normalise, making a career in cyber security, something that people would aspire to and also making it clear that it isn't just about Sort of, you know, for those people that want to spend time doing deep analysis of technical issues. Yes, there's a place for those people irrespective of their, you know, their gender or whatever. Yeah, but equally there's this whole sort of raft of stuff that needs, sort of, needs skills that didn't come from the traditional cyber kind of catalogue, if you like. And I just think that as it's mature all over, but certainly the last five years I've. Seen a huge change. And I now do see, I mean I do quite a lot of speaking at universities and this kind of thing. And I do see more diversity in the room than I've ever seen before, so I think, yeah, I think we are slowly but surely making an improvement in that space. And I think it'll look very different 5 years from now, when we look back.

**AB**

No, I would agree with that. Thank you for that Paul and what advice would you give to those that that are looking to embark on a career in cybersecurity?

**PV**

So, there's a lot of resources out there now for people to look at. So, so first of all, if we're talking about people who are still in school then, and so maybe haven't yet decided where they want to go to university or go down the degree route or whatever, then I would say there are. You know, there are some great websites that you can use as a resource. There's actually the fairly newly formed UK Cyber Security Council. Sounds kind of quite sort of daunting when you say it out loud.

But it. It is actually. They're starting to build kind of career Road maps and things like that, which I mean, they mentioned things like Cyber first, which I know you just mentioned before, which I think is a brilliant initiative, by the way. There's also a website called Cyber Choices which I think is a good website to look at as well. You know that’s got. More of a kind for people who want. To kind of start to let's just say play at cyber related stuff. But they want to do it in a way that's safe and doesn't expose them to anything illegal, for example, and also talk to, you know, talk to your teachers about this stuff. As well because. You know, there's more and more material available.

And then for those that, say, have decided to go down the sort of higher education route and go into sort of degrees and that kind of stuff. Again, there's lots of specialist degrees available now specifically around the cyber topic. Historically, we would have come from a computer science background. But it's not essential to do that anymore. You can actually sort of do a degree in cyber, but there's loads of degrees in Cyber I know in Lancaster, do quite a few of these as well. So yeah, it's one of those things where there's, now, you're almost overwhelmed with choice. Actually, it's the truth of it. But I think that's a good thing. I think I'd rather have more too much choice than too little, so I think that's a good thing.

**AB**

That's a really, really good point and just kind of touching upon, as you mentioned these kind of specialist degrees within kind of Cyber-Security. More recently, I kind of attended a cybersecurity symposium here at Lancaster and that was kind of partly set up to announce the newly launched Cyber Security Executive MBA. And it was a really kind of fascinating debate and kind of discourse that took place on the day surrounding kind of cybersecurity leadership and whether cybersecurity leaders were expected to come from. Kind of technical background or whether they had to, you know, just be curious and willing to learn. So, I kind of wanted to get your opinion on this, given that you are kind of the technical director for NCC Group. Do you think that it's important for kind of cybersecurity leaders to be from a technical background, or is it that kind of openness and willingness to learn that that is required, that can potentially kind of overcome, perhaps not coming from a technical background?

**PV**

So actually, in my sort of day job, I deal with cyber security leaders all the time. Actually, that's pretty much my all my customers and my clients that I deal with on a day-to-day basis are cyber security leaders and what I would say is that there is an incredible range of backgrounds there, and that's partly because of the, as I say, the demographic is such that when a lot of these people started their careers, it was still very much a new thing. So, people came into it from lots of different backgrounds. But I would say that there's no material difference that I've ever observed between someone who's a good lead, a good cybersecurity leader, whether they're from a technical background or from a non-technical background. So, what I think I'm saying there is that the skills and the abilities To be a good cybersecurity leader don't depend upon you having a strong technical background. That said, I do think that some exposure to technology is probably helpful. I don't mean a technical background as such, but just an essential understanding of some of the sort of topic areas. It's probably important. I do actually think, though, that most cybersecurity leaders, their biggest challenge day-to-day, is engaging with their business, you know, with their business colleagues.

So, getting the message across into the business, getting the business to sort of do the right things if you, like, from a cyber security point of view, from a cyber resilience point of view. The biggest challenge they face is actually dealing with that audience, and so therefore they don't find, in my experience, they don't find themselves dealing with super technical things. You know, on a on a regular basis and actually to be coming from strong technical background or especially more exclusive technical background could even be a disadvantage. Because it may be that having some of that more business sort of understanding is potentially an advantage if you want to ultimately become a cybersecurity leader. So now I would say. It takes all sorts as, as I said before. And I think that the best sort of cybersecurity leaders. That I've come across do have a grasp of some of the technical matters, but don't feel the need to become deeply sort of embedded within the technical side of things and are much more interested in that. Essentially in managing. You know the problem. For it, so it's more of a management skill set I would say.

**AB**

Now it's really interesting to get your kind of take on that, given that you know you work with several kind of leaders within kind of the cyber landscape. So, thank you for that, Paul. The next question I had is probably kind of one of my favourites given that I am a huge fan of the show, channel 4's Hunted series, it'd be great to kind of get your take on that. In terms of kind of how that opportunity came about to actually kind of work. As part of that. And also, kind of from a cyber angle kind of what you do. I believe it's head of Cyber that you have taken up that role as part of the kind of series. But from a cyber angle, is it kind of in terms of kind of the work you carry out with the fugitives? Is it, is it kind of an element of social engineering that you do to try and kind of to delve into the psychological aspects of the fugitives? I know that for a lot of us technology and social media can be our weakness. We spend a lot of time kind of scrolling through and kind of sharing our day-to-day lives on there. So, I just kind of wanted to get kind of stuck into kind of what it is that you what you do on the show? And the techniques that you use as well.

**PV**

OK. I mean, so, yeah, I mean obviously this is one of those things that it came along in sort of what 2014? I think it was. I never realised when it came along that it was going to be something that I was going to be involved with for several years to come. It struck it, you know, it seemed like a one-off thing when it first emerged. What basically happened was we actually got approached originally by a journalist. Claudia Joseph and she was doing a piece on what it would, what it was like to be hacked. And as she approached us and said basically, I'd like you to hack me and I want to write about it. And so, we sort of, to cut a long story short, we did it, we hacked her and she wrote a piece about it and we thought that was kind of that was that and then what happened was it just coincided with the research that was being done. To look at this new show, which ultimately became hunted, and they approached, as in the TV company approached us and said would we like to sort of get involved and initially we thought we'd be advising on the show and then it turned out that actually they wanted us to sort of actually do this stuff which was exciting and a bit scary, but actually we sort of went ahead.

And did it and what was interesting about it was when the show started the very first season of the show, it wasn't really a game as such. There was no prize money. It was seen as what they call the social experiment and so we were really interested in exploring that and this. It is really where the book came from, because it turns out that it's the digital footprint stuff that is the that's the thing that we exploit. Essentially when we're doing the show and so what we what we do is we essentially do incredibly deep research on the individuals. Yes, we do gain access to their social media sites and things like that. We often gain access to their devices, things like phones and laptop. And so, a lot of the work is as much digital forensics as it is cyber. But the two things are sort of enmeshed any way. It's all become part of the continuum. And so, yeah, we do a bit of social engineering we do, we don't do anything that I would call traditional hacking. We don't use things like so-called zero day exploits or anything like that we typically, because there's all sorts of you've got to understand, we have to stay on the right side of the law. There's all sorts of permissions required to do these things. So yeah, you know, we can't just run Riot on the Internet, that that would actually that would cause problems. So, but that all said, we do. There's a huge amount of effort that goes into making this show ‘fair’ in quotes. To make sure that we only can do the things that we would be able to do in the real world and so to some extent, we sometimes feel as though we have one hand tied behind our back, but actually it, it does make for a better show and it makes a better, TV. And yeah, we thoroughly enjoyed it, and as I say, the one thing that I really took from the first couple of seasons of the show was that people have these enormous digital footprints, where they expose huge amounts of information about themselves online, and that sometimes just in the public domain and sometimes you know you have to actually get into their accounts to see it. And nevertheless, there's a vast amount of information that's out there, and that's often enough for us to be able to start to anticipate what their next move is going to be or who they're going to contact that kind of thing and that's how we sort of do the things that we do on the show. We basically delve into those digital footprints. I mean, of course there's other aspects to it. If you've seen the show, then you'll know that there's other aspects to what we do in the sense that there's people on the ground interviewing people in sort of more traditional way, and they're doing things like accessing their devices while they're in their homes. And that kind of stuff. So yeah, all in all it becomes quite a... It's very exciting to be part of to be quite honest with you. You kind of lose yourself in it while the shoots going on. It takes a few weeks and you are literally living in a bubble for those few weeks and you become very invested, I think is the right word, Into the whole outcome you sort of lose sight of the fact that it is a game sometimes.

**AB**

Yeah, I can only imagine. I think that it's really interesting in terms of kind of the celebrity and non-celebrity dynamic as well. You know, having watched kind of both of those and I think you can probably best speak on kind of actually you know having to deliver on the show. But in terms of kind of with celebrities, they have kind of an abundant network and possibly even an abundant net worth too, which means that they can often kind of pull off the unthinkable. And comparing that to kind of the non-celebrity who may not have as significant a digital footprint and so can kind of stay under the radar. So, seeing that kind of dynamic in play is really interesting as well. Has there been anyone on the show, a fugitive that has kind of struck your interest based on kind of their approach?

**PV**

Well, there's been some fantastic approaches taken. So, I mean a few, spoilers, I suppose, because everyone has not seen the show but some of the ideas actually that some of the fugitives have had to sort of stay below the radar have been quite impressive actually. As early as season 2, the two of the fugitives that won the show were using canal footpaths as a way of getting around the country on bikes. Which was actually a stroke of genius, because there's almost no CCTV you know, on those kinds of things. And so, they were pretty much just off the radar for huge amounts of time. And that was again, a stroke of genius really. There's been a few other examples of that kind of thing. We've also had a few fugitives of the non-celebrity type trying to play the cyber game a little bit and try to sort of use technology while they were on the run, I have to say that that nearly always backfires the moment you know to do that in a way that keeps you completely off the radar is exceedingly difficult. You have to have an extremely rigorous operations security and most people; most ordinary people don't have that. So yeah, they tend to sort of show out quite quickly when they do that. But actually, most people seem to go rural these days. They seem to sort of realise that getting off the grid is the is the is the right thing to do. Of course, the one point I would make is actually as you know, if you've seen the show, is that often it isn't the fugitive’s own technology that exposes them. It's the people they're connected to, so it's actually their friends, their family, the people who are. Helping them. It's often their technology, their phones, their laptops, their CCTV cameras that are actually the weak link. That that allows us to find out where they are, so yeah.

**AB**

Yeah. There's so many kinds of layers and factors to it.

**PV**

We keep going back for season after season because although technology moves and shifts and changes as well, so new ideas come up every year and we have new ways of hunting people and equally the fugitives have new ways of dodging us. So, every year it's exciting because there's new ideas. And then we started to use in the last few years, we started to use you know the telemetry that's in vehicles and stuff like that as a way of being able to track cars and when they're on the run and stuff. So, all of which of course is real. I mean these things exist, that is data out there in the real world that is available to, you know, law enforcement under the right conditions and these things are incredibly sort of powerful. This is very, very difficult these days to stay off the radar. If you've got the right level of law enforcement coming after you.

**AB**

Yeah. Yeah, no, absolutely. Thank you so much for kind of providing more insight into the show. It's always good to kind of get some more kind of context, you know, on what kind of goes on behind the scenes. Obviously, when you're watching it from a kind of an entertain entertainment kind of value point of view.

**PV**

Yeah, I mean. There is a slightly serious angle to it too, you know, to pick up that point there is a serious angle to it and that is a lot of the stuff that is, that people are or that they're doing to people is all to do with the fact that they've left all sorts of information lying around on the Internet that we can use against them and that, as I say, that's what sort of inspired me to write the book because I realised that most of us were putting that stuff out there far too easily and actually just a few. A little bit of thought a little bit of not even very much in the way of technology to be honest. You can actually dramatically reduce that and make yourself much less exposed. Used to those types of risks, and so that was the slightly more kind of serious edge to it that, you know, this whole social experiment thing, which happened with. The first season. We came away from that thinking, OK, there's some stuff we need to help people to manage this stuff and navigate this stuff because it is bewildering to a lot of people you know.

**AB**

And just to finish, Paul, I think this is a nice way to finish, but in terms of kind of you know the future of cyber and the kind of cyber landscape, how do you see that kind of unfolding in the future? I know particularly in the north, there's a lot of development taking place. Of course, the National Cyber Force set to be based here in Salisbury and you know a lot of universities as well. Cyber is very much on their radar. If we look at kind of pedagogy and we look at the courses now that were available, there's a lot going on as part of this kind of cyber ecosystem. But how do you see that cyber landscape unfolding?

**PV**

Yeah, I mean it well, you know again that there's a huge amount going on at the moment as you as you've pointed out. I think there's quite a lot of. So first of all I would say that if you take cyber. It's wider sense just to start with so Cyber is now typically business and cyber and inextricably linked because almost many, many businesses now rely on some kind of online presence. And so, you know, it's going to become even more intrinsic and important to businesses in terms of getting this right going forward. And so from a general point of view, as technology changes, cyber changes. Yeah, and we're gonna get more and more kind of things like Internet of Things and some of these other things. And there's already been some interesting things around that with things like ring doorbells and some of the other sort of the vulnerabilities that have appeared over the last couple of years that's going to increase so. And there's a lot of legislation regulation that are coming around that too, which is a big opportunity for people who want to work in the industry because there'll be more  need for that type of those types of skills to come in and manage that so... So that's all good and so I think that it is going to become more business as usual. And it has been. It's seen as very specialised to begin with. It's seeing it being seen as less specialised now in terms of what I mean by that. We don't need deep specialisms to get into the industry and I think that it's going. That's just that trend is going to continue. We do always need those deep specialisms, but the industry itself is much bigger than that, you know much broader, so I see… it's exciting times. I mean, there's stuff coming along at the moment around the idea of digital identities and all sorts of thinking around how that's going to become the new kind of things. Like, you know, the death of passwords. That have been... It's been talked about for a long time, but I do think that we can start to see the beginning of that.

Now we can start to see how the way we interact with businesses and with our web with websites and with mobile apps and it's all going to change and that's going to have a significant effect on the cyber security side of things as well, so it's yeah, it's really it's a really interesting time at the moment. And I think the next five years are going to be, you know, it's going to be a lot of change and also of course the threat. You know, I haven't, we haven't mentioned threat at all really in this in this session. But you know the threats growing all the time. Governments are using this stuff more and more for against other governments, criminals are using it more and more, you know, to make money. So, we are going to see much more. We've probably all had dodgy texts and dodgy COVID messages and dodgy emails coming through, you know, thick and fast and dodgy WhatsApp messages. You know, I mean, we're all getting used to that now and that's just an indication of how much more criminals and stuff are starting to use this as their sort of as their first choice of how to extort you from your money basically. So yeah, I think it's going to be a very exciting time for next few years.

**AB**

Yeah, absolutely. I think equally as much as it is exciting, as you mentioned there, you know the cyber threat landscape is very much kind of in full force and that's something of course that like you said, we are becoming kind of accustomed to. And something that we need to be mindful of. Thank you so much, Paul, for, you know, taking the time and agreeing to kind of kick start the Demystifying Cyber podcast. it's been a pleasure. So, thank you.

**PV**

I thoroughly enjoyed it. Thanks Ajay really, really. Really good to chat.

**AB**

Thank you for listening to the Demystifying Cyber podcast. We hope you've enjoyed today's episode. Feel free to get in touch to find out more about the Lancashire Cyber Foundry. Join us next time to further unpack and demystify the cyber landscape.