Chris Hurst & Iain Johnston of Blackwired

Interviewed by

Jane Bird

17 May 2022

Via Zoom

Copyright

Archives of IT
(Registered Charity 1164198)

Welcome to the Archives of Information Technology where we capture the past and inspire the future. It's Tuesday 17th May 2022 and we're talking on Zoom, as has become customary during the coronavirus pandemic. I'm Jane Bird and I've reported on technology and IT for newspapers such as The Sunday Times *and the* Financial Times *since the early 1980s. Our contributors today are Chris Hurst and Iain Johnston from the cybersecurity company, Blackwired. Chris is currently Blackwired's Chief Information Officer and Chief Information Security Officer, while Iain is founding partner and Managing Director of Blackwired in the UK and Europe. Blackwired is bringing military cyber countermeasures and adversity disruption to the enterprise sector. It's currently engaged with the UK government and leading law enforcement on the future of oversight and attribution in crypto markets and cybercrime. Chris was previously a leading security practitioner at BT where he acted as the virtual CISO with BT's largest clients. He was also head of security services, principal architect in identity and the inventor of Fedcore , a federated industry management capability which became the model for the UK government Identity Insurance Programme.*

Chris and Iain, welcome, I'm very much looking forward to hearing more about your experiences and insights into the world of cybersecurity and the dark web.

Both: Hi.

So, perhaps we could begin with how you got into all this, Chris. I know we don't want to go a lot into your personal background for this interview, but maybe you could give us a short synopsis as to how you arrived where you are now?

Chris: Oh, absolutely. So I've always been interested in computers from the last days of school where I was in a computer club, they were building them actually, and through periods of time I've gone through software design, product design, obviously into the security domain, and finally into cyber and into cyber because it's an area that I felt that needed new concepts and that's what I kind of positioned myself to do because I like to look at big problems and provide solutions to big problems, and cyber is certainly a big problem area, as is crypto. So that's how I got here. I also got here by meeting some great people along the way, some from the information

technologists' group; Vint Cerf, for example, the inventor of the internet, and Tim Berners-Lee, the inventor of the worldwide web, and spoke to them about the identity Fedcore program and how that would be the next organising principle for the internet's whole identity. So I'm always pushing the outside edge of the solution space or the edge of the mind map.

Thank you very much. And Iain, how about you?

Iain: So I got into technology later than Chris. I got involved post the military and have been working in technology for twenty years, increasingly towards payment security, ID security and now cyber. Chris and I worked together for twenty years and he kind of coaxed me out of the military in the first instance and it's very interesting what we're doing just now has shades of military tactics now applied to the cyberspace.

Thank you very much. So let's look at the dark web, if we could start there, what is it and what goes on there, Chris? Could you shed us, shed some light on this mysterious topic?

[00:04:10]

Chris: Yes, I can. So if I could contrast the dark web with the light web, that'll probably be a good place to start. So the dark web and the light web actually almost started on, you know, at the same time. So the light web began in 1989, if you like, with the worldwide web, obviously Vint Cerf developing for DARPA, which was ARPAnet, which was actually a military application, a joint project with education including UCL London but also the US Navy. So that's where we get our internet protocol from. And basically the light web is, as we know it, it's open, it's searchable, you can use a standard browser and you can get around, it's indexed and it's robust. And it was the robust part that Vint Cerf was looking for, because he wanted to make sure that if there was any attacks or disruption against communications in the US, then that communication would still be delivered by different routes around the network, the internet. So if I look at the dark web, it is effectively a closed, unsearchable area of the same sea, ocean of ones and zeros. So

basically, that same ocean we swim in, it's the same ocean that's used by the web, but - it's ones and zeros, it's the same – but it's closed and it's unsearchable. So it's not I indexed and it is cloaked. So all communication within the dark web is encrypted, enciphered and as there is no indexing or there is no searching in the dark web, in effect you have to have, you have to have certain bulletin boards for reference where you can go to access the dark markets. And this is, this dark web is an industry, so it is an ecosystem that exists in a parallel world to the light web, or the world that we actually live in. So dark web, it's a parallel universe to do certain things, so there's marketplaces, there's communications, there's messaging and so forth, but it's all obscured.

[00:06:51]

Yeah. and so why is that dangerous?

Chris: Well, it's… you could say that both light web and dark web are dangerous in of theirself, because it enables, you know, the very rapid passing of ideas and at the same time it enables a certain attack surface. You know, so we look at social networking and so forth, we look at internet and things, they're all on the light web and they are dangerous because anybody in the light web can access those things and look at your baby monitor and all that stuff. So I think danger is all about the difference of purpose of the two networks. The light web, the purpose is to provide access to content, access for commercial purposes, legitimate stuff, but also it has a side which has recently come to the fore where it's actually being used to do different things. So there are websites for, you know, people trafficking, child grooming, sex trafficking, those kind of things. They're in the light space generally. So in the dark space it is effectively, as I said before, a closed space, so to participate in the dark web you have to have certain browser, the onion browser, you have to…

Sorry, a what browser?

Chris: The onion browser tool. Yeah, so it's a different type of browser. You can't browse the dark web with Google Chrome or Microsoft Edge or any other ones, so you have to go into the tour with onion browser, so it's a special type of browser.

So… and in effect what happens is there is an industrial complex behind that, there's no other way to put it, and I'll talk about that in a moment, but there is an industrial complex. Loads of things you can, you can do some legitimate things related to crypto, which is absolutely fine, but you can do some illegitimate things related to cybercrime, terror and so forth, drugs, weapons, those kind of things that you would not see marketed on the light web. So all that goes on in that closed space. So it is dangerous, but as I say, the surface web or the light web can be a dangerous place too. But just to be really clear about this, the reason I'm involved in this and the reason I'm in this space really is that all cyberviolence – and I'll come on to that in a moment – is planned and prepared in the dark web, yeah? Out of sight, unobserved and basically encrypted. So there is little or no identity or attribution within the dark space and effectively there is no transparency over it. [00:10:19] So there is a key difference between the light web and the dark web, is that on light web we have transparency, it's in the sunlight so we can see who's doing what to whom. In the dark web we do not. But the most significant thing is what I see as – and I'll come on to this just in a moment – a crossing of the Rubicon and also a break cover aspect of the dark web. So, as I said, most of the cyber violence is planned and prepared in the dark web. Yeah? Most of the execution of that violence and the effects of that violence is felt through the light web, so the internet, networks and so forth. So in effect, there is a pernicious element which has become an industrialised element, and I'll talk a bit more about that in a moment, of the dark web. And that is where organisations are industrialising their attacks; they're creating weapons, they're buying, selling and trading weapons, cyberweapons, zero-days, and what they're also doing is creating the infrastructure to launch those attacks, maybe forward operating bases as we would call them in the military, but basically they are intentionalities to say I'm going to attack this organisation and I'm going to build these components to do that, yeah? So they'll be, interestingly, in the light web. So you'll have a public facing IP address, yeah, you know, from which a cyberweapon is being launched, or malware is being delivered, or ransomware attacks are being delivered. So if you think about it as kind of a dark space, yeah, and a light space, yeah, in effect we need transparency in the dark space, which is what I'm about. We also needed that transparency in the light space. And transparency forces a number of questions on us. What ethical questions, what moral questions, what human questions do we have to have about privacy, about surveillance, about all those kind of things, you know, in

the light web, but also, what if we don't have transparency on the dark web. And, you know, that's a critical issue I think for, you know, for modern times. So we can't currently see that, with one exception, but I won't bring that out, though Blackwired does that. So we specialise in the observatory of the dark web, the dark space, so we look at that intentionality for bad actors, bad actor groups, the construction, if you like, of infrastructure and bases and cyberweapons, including malware and phishing, phishing attacks and so forth. So that's where we are. What's generally attacked, though, Jane, from the dark space and by bad actors is the systems and processes of management control. So what we're seeing, what we're seeing and we've been seeing for some time, and I'll talk about one of those Rubicons that were crossed, we've seen attacks mounted against production facilities, you know, aluminium alloy production in Norway, distribution facilities, the… an attack which had a lot of sideways problems with a file transfer service, a file transfer application called Accellion, and again, distribution Solarwinds, which is obviously a distribution, a tool designed to explore and gather information about networks, but obviously you connect it, and something that was good becomes something that's bad because it gets exploited by the bad actors in the dark space. So the three things that are attacked are production, distribution and exchange. So, banks, stock exchanges and so forth. [00:14:57] So this Rubicon that was crossed… this Rubicon that was crossed, in 2010, August 2010 the Pentagon declared that there was a fifth domain of war fighting and that was cyber. So there's been a fifth domain – obviously land, sea, air, space in the US concept – but now cyber. And that's in recognition of the fact that – and that's with the genesis of Blackwired – is that cyber, all the preparations, all of the planning is done in the dark space and the Pentagon said, okay, well look, we're being surprised too much in the light space, we need to organise around and create a cyberwar fighting capability. And generally that was in response to the fact that they couldn't see what was going on in the dark web. So what happened also in 2013 is that one nation state attacked another with a cyberweapon and that cyberweapon destroyed national infrastructure. So that's the first example of what is a kinetic result…

Which countries are we talking about there?

Chris: Well, we're actually talking about the disablement of the Iranian nuclear programme and the general attribution is thought to be obviously the US, but that is

the Stuxnet, the Stuxnet event in August, and that is the first time, and this is questioning – Michael Hayden who was the Director of the NSA at the time – questioned, questioned the morality, the ethics and the possible consequences of the use of cyberweapons at that point. So Michael Hayden and the group around him were examining those very things that I talked about in terms of transparency does force you to question, yeah, to question what you're doing. So that was a really significant Rubicon, right? So one nation attacks another one in a time of peace. Yeah?

So his question was whether it was legitimate to pursue this, I mean like you might say, well, we shouldn't have weapons of mass destruction, that he was saying, well, we must ask ourself, should we have weapons in this fifth zone.

Chris: Yes. Well, yeah, indeed. So having declared that fifth domain in 2010, effectively that opened the door to all of those questions about transparency, certainly on the dark space and the need for it. So my, you know, my view was obviously looking at being, you know, somebody involved with Vint and Tim Berners-Lee development of the internet and what would be the next organisation, sorry, organising principle of the internet, which is identity, where it comes from, the identity insurance program as you mentioned, you know, so Fedcore , is around that, so discussing that event. I firmly believe that once we've made that leap from, you know, worldwide web, the next leap, if you like, for the internet will be identity and transparency on that would force a number of questions into the open, yeah? So how much of your identity are you fragmenting and throwing out into the light web? Yeah? There's some big questions there that I got involved in and I provided some solutions for those things, but if you look at it in terms of the dark web one of the biggest issues is going to be, is going to be attribution and basically any kind of enforcement, yeah? So we do have a number of issues that are really at the heart of where we go with these things and I think the dark web and the crossing of the Rubicon between military grade fifth domain war fighting and bringing that into, bringing that into the enterprise sector, because the enterprise sector is, you know, producing things, you know, making tea, making aluminium, making ice-cream and also distribution, so logistics, aircraft, ships, you know, transportation of stuff, and exchange, obviously, you know, the monetary systems. So they've all become

unfortunately targets for violence, cyberviolence. So there are three types of violence that I see. There is instrumental violence, which is I want some money, you know, it's ransom, yeah? Or extortion. So it has an instrumental piece and you see the headlines are everywhere in terms of ransom from, you know, running from Colonial Pipeline through to other organisations. But also underneath that there's what I would call expressive violence, yeah? So expressive violence is really, is really looking beyond the instrumental violence of let's say a ransomware attack or an extortion attack on the Colonial Pipeline, but actually, what was that, what was the expression behind that attack. Was that, you know, was that expression of control over distribution, yeah?

Yeah.

[00:21:25]

Chris: Yeah. So interesting, that's where we're going. And the last one obviously, which has been pretty recent, which is statement violence.

Such as?

Chris: Such as a statement violence, the Sony Pictures attack where North Korea attacked Sony Pictures in retaliation of the release of the film *The Interview*, which is, that's a Rubicon that's been crossed, if you like, where North Korea state attacked a public company, Sony Pictures, in response for the movie, *The Picture*… or *The Interview*, sorry. And also you have, you also have another attack which came in 2016, which was an attack on the Australian defence and government. That was done via a public company – a private company, sorry – called NewSat Ltd, and that was one called out, again, by Michael Hayden as a crossing of the Rubicon, which is where private companies and enterprise have become part of a cyberwar.

Yeah. So, right. So these obviously are all quite significant threats, enormous threats potentially, and I suppose the question then is, what can be done about it?

Chris: Yes. Yes, so indeed, what can be done about something that is planned, prepared in a dark space that you can't see, and then it appears as a surprise with some gory headlines about, you know, Colonial Pipeline and that kind of stuff, those breached named as [?,] and so on. So what we can do about it though is we can take the stuff that's been learned in the last twelve years from the cyber warfare battle space. So we can take those lessons and they have been taken on by the Five Eyes, the intelligence community globally, and they called out last year the biggest actually threat is actually going to be, is actually going to be to those organisations, private organisations that produce things, distribute things, exchange things. So they have become targets for that expressive and statement violence by other states. Yeah?

Can you just clarify the Five Eyes, what do you mean?

Chris: So the intelligence community consists of the MI, so the military intelligence for the UK, US, Canada and others actually comprise the Five Eyes, yeah? I just gave you three of them, but that, you get the picture. So actually last year – and we saw this, you know, in Blackwired in terms of Zero Day Live, what we saw from around 2016 is a huge increase, a huge increase in the development of weapons and the preparations to act. We saw huge uptick in…

[00:25:14]

Can you kind of give some examples of that?

Chris: Yes. So in the preamble to the Ukrainian War we saw cyber, we saw cyberweapons created for the first time in 2022 at a rate of five per day. So those weapons were aimed at either spyware, disruption, denial of service or that statement violence. We've also seen that used on both sides in that conflict, and this is obviously public information so that's not something that, not something that is secret. But we saw actors switching their – dark space actors – switching their, switching software, software switches to open their weapons for the use of former CIS states, yeah? And we saw weapons used to gather up in preparation, in December, for the gathering up of thirty-five million Ukrainian identities. Obviously with my identity we'll be looking at that and thinking right, okay, well, that's a, you know,

that's a very interesting preamble to any kind of invasion, so you have to know the people that you're invading. So those kind of things obviously relate to [incomp 26:45], we've also seen the development of polarised groups. So Russia, obviously, you know, Russia and Russian groups reforming, forming, making alliances, creating a development pathway for their weapons and their infrastructure to do a number of things. And this, by the way, I'm not singling out the Russians here, that there are other nation states that are doing that, but obviously they are private groups within those nation states that actually earn money from this. So we can see that money developing, but we can also see changes in their planning and their preparation that indicate that things are going to be attacked, we can see that directly from our platform so we've seen that uptick of Zero Days. So a Zero Day, if I can explain it, is something developed in the dark space that is actually an integrated weapons system rather than just, you know, a piece of code. So it will enable you to automatically launch a ransom attack or a denial of service attack or any other kind of attack, a spyware attack actually, or an attack on exchange, a bank or whatever. But these are industrialised, robust, working weapons that are continuously developed, at a speed that our light web capabilities or our enterprise capabilities cannot possibly hope to achieve parity with. Yeah?

Okay.

Chris: Yeah. So what I'm looking to do is to kind of redress that balance, because there is a very particular direction of travel that I've taken with Blackwired and Zero Day Live to produce prevention as opposed to detect some response, which is the general process of the way that we look at things. So, as I mentioned right at the top of the interview, I would look at why does the world need new concepts, yeah? Because the old concepts are worn out, we've not adjusted them, we've not looked at them since 1989, 1990, so we really haven't. We also, my interest in regulation and compliance from my role as a CISO, is that we need to develop better regulation, but the only way we can do that is to get oversight of the data space, certainly in the dark web and also in the light web. So we need to know what the data space is, otherwise we can't develop, we can't develop compliance notions, we can't develop enforcement and we can't deliver consequences to those people that perpetrate the crimes, if you like, in the dark space. [00:30:10] So it's a very interesting, complex,

fast moving, difficult and hyper-connected space, yeah? And I just want to make the point that those particular, yeah, the light web and the dark web is the same ocean of ones and zeros, which makes that whole space interesting. So I sometimes talk about a red ocean of ones and zeros. I can only, we can only see and experience less than fifty per cent of it, which is what the light web looks like, the other fifty per cent we don't see and experience.

That's an extraordinary idea, isn't it? Because intuitively if there are bits and bytes, noughts and ones flying around the world on optic fibres or going through sort of radio signals or whatever, you know, the idea they can't be intercepted is counterintuitive.

Chris: It is, it is.

How can they exist if they can't be…

Chris: Yeah, it is counterintuitive and I think that's the, that's a piece of thinking I've been doing in a little series called 'In the Future', and I just, I just looked before this interview, I wrote in 2017, yeah, 'In the future extremely complex tightly coupled systems and ecosystems will suffer the equivalent of a force ten storm that will destroy it', yeah? 'The high speed volatility we're experiencing are the harmonics that precede that storm.' So I think that, you know, so what I was trying to look at, you know, I was looking ahead here to say how can we get transparency, how can we develop preventative capabilities, how can we prevent identity attribution and so forth. That's where I was looking. Yeah, that's…

So there is, there is a potential there, is there? It strikes one it's a little bit parallel to the climate crisis in a way, you know, is it going to be Arma… you know, is it the end of the world? I mean it sounds…

Chris: It is. It is and I want to, you know, I want to look at that because I'm interested in those big problems and those big problems require you to have, to observe a huge dataspace, but also then look at what connections, what – how to put it – what determinism can you allocate to those changes. So, for example, in climate

change you have weather systems and so forth and you also have geological systems that might cause problems. So what do you do with that information, what do you gather up, what do you learn, how do you create it? And if you look at those things, you know, when we do put geological sensors and information gathering nodes, if you like, to provide us intelligence knowledge and other things about what's going on. Distance inside a volcano, for example. Why not apply that kind of philosophy to the dark web, yeah? That's where I'm going. So what I think has happened, and it's going to sound very strange, but I think that we've got concepts of operations that – I'll just use another military term – that were good for 1990, or 1989. They're not good for 2022. There's a lot of space between 1989 and 2022 for stuff that happened at midnight when you weren't watching or you could not observe, and that's what's happening in the dark space. So if you like the spontaneous flash of disruptive insight, yeah, that we're providing in terms of Blackwired Zero Day Live, is we're looking that way, we call it Left of Bang, right? And the reason we did that is because of, we knew that traditional military doctrine and methods, processes and management of battles was failing in Afghanistan and the US Marine Corps Hunter program actually looked at what are the fine grain things that we can find out, you know, who's standing where, who's watching what, who's building what, who's buying plastic tubing to put IEDs in, who's buying different electronic components and mobile phones, who's doing that. So these are all preparations that we couldn't see before. So the Combat Hunter program brought those things into the sunlight so the real actionable intelligence could be, you know, could be created from that. So, don't do this, do this. Save lives, don't get ambushed, don't get attacked, yeah? So I looked at that philosophy and spun it round, if you see what I mean, to look at cyberspace. Less, you know, just because the dark web is closed and unsearchable, not indexed and cloaked does not mean that you can't get inside the dark web, yeah? You don't have to see inside the volcano to see what's going on, you plant a sensor.

[00:35:46]

Say that again – you don't have to see inside a volcano…

Chris: You don't have to see, you don't have to see inside the volcano to know what's going on, you just plant a sensor in it, yeah?

Yeah.

Chris: And it tells you, it tells you what you need to know.

Iain: Could I interject a couple, just on a point, the, Jane, where you're trying to get to is the sheer scale. The thing about the Afghanistan that Chris refers to, despite the fact they were clandestine tactics it was still very much in the light. What Chris is kind of illustrating here is the sheer scale of the dark web, the, you know, these are industrial complexes, The Conti Group has their own building and an HR department and approved the use of weapons, as Chris is describing, for use against certain other groups. You know, it really is very industrial and yet we don't see it and I think there are those that still have a perception of it's largely amateur. It's not amateur and the pace at which they operate, Chris's 1990s point was, if we don't react in the same way that military forces had to react differently in the thirties when they saw Nazi Germany finally building up its resources, we don't react soon there will be an overtaking of events. During Covid, for eighteen months the level of resource that was assigned to working in the dark web tripled, because people were working from home, they weren't getting paid, so they went and did other things. So I really just want to re-emphasise the point Chris is making about the scale of the dark web and the enterprise that's sitting behind us, facing us, there needs to…

Are you saying that there are bricks and mortar, and, you know, in the end the money has to come out somewhere, doesn't it, are you saying that, I mean they can't be totally…

Iain: Resources need to be applied to… Absolutely.

Chris: It does. Absolutely, that's what we're saying, yes.

Iain: Resources need to be applied to countering this with, in equal measure. The scale of technology that's coming in our direction, the cyber teams cannot be recruited fast enough, they can't build capability fast enough to match what's coming in the other direction, so there needs to be a real recognition that, you know, we are in, Chris

uses the term, we're in an arms race, and we're not producing responses at the pace at which the adversary is operating. And the other element to that is that the enterprises who are hacked and otherwise often don't fully declare the picture. So you've got two things happening, is we don't see what's coming in our direction from the adversary fully and we also don't have a declared position. You know in Afghanistan if a soldier dies or if somebody's been injured. Much of what's happening in cyberspace is not being declared. Increasingly that is changing, but much is not being declared.

Chris: It's not being declared, absolutely.

Because banks and financial institutions and so on don't want to admit that they've been hacked, you mean that sort of thing?

Chris: Yes. There are, which is the next part of where I was going actually, is that, is that there is no, there is no black box flight recorder on businesses to tell you what's actually happened. So, or what's happening, actually. So again it comes down to, you know, how much transparency and how much can you observe of what's going on in the dark space and how much you can observe of where what goes on in the dark web is actually caused or is causal of violence, you know, in industry. [00:39:54] So it's, it brings us into a couple of things really that also as a data scientist I'm interested in, which is how much do we know about the size of the infosphere that is actually in the dark web and, you know, what data is there there that we can use. And the approach that we've kind of taken is to look at, is to look at that problem in the same way that we would look at the human genome project, or the human protein project, which is mapping that and providing data and information from that. So if you look at it, the way that this thing is working is very much, you know, bioscience, yeah, or life science because of the complexity in the interconnections. So what we've looked at is, yeah, what are the components. What are the things that we need to see, yeah? How do we get to see them and how do we monitor, and how do we turn that knowing into action, yeah? And two kinds of action. One is to inform regulators and authorities, which we're working with at the moment, about the risk, the size of risk that they have, and the other one obviously is to defend enterprise, because the enterprise is largely on its own, it's spending an

awful lot of money at a time when there's not an awful lot of money to be had, and organisations traditionally have said, well look, you know, cyber attacks, cyber problems, you know, they're not my problem, they're GCHQ or they're MI6 or MI5, they're government's problem, they're law enforcement's problem. But actually, you know, we're not doing that well, so we're looking to provide that oversight, that observatory and that dataspace necessary to deliver that view on which you can make better regulations and understand what's going on. Because what we're seeing is, or why I said 'In the Future', just another one was countries will legislate on data accountability transparency and reporting, yeah? They will actually legislate that. So that's compliance with enforcement. Right now we don't have much of either.

Right, yeah.

Chris: Yeah? So one of the issues is, I guess, you might, you know, the military might have in Afghanistan is they do have enforcement capability, right? They need to have it so they can go and, you know, they can go and disrupt the, go and disrupt the adversary, you know, make sure the event does not happen, and you don't have to kill people to do that, you just have to not be there, if you see what I mean. Yeah? So I think we're approaching a very interesting period in cyber and information technology where the technology is moving so fast. For the majority of time that technology is driven by economic means, and that includes cybersecurity, yeah? It's become, it's actually become applied economics because businesses cannot afford to continually invest at the level, let's say, that the US Sixth Fleet does at 600 million US dollars per year in cybersecurity, or cyberwarfare actually. So what we're trying to do is to actually bring that thinking, and it is a thinking change, it's a sea change in the way that people look at things, bring that thinking to the enterprise. Obviously our origins is military so, you know, it is actually in that conflicts part. But I think there is a, you know, that force ten storm is coming and I do believe these are, you know, this is the portent of it, but what we've done is we've created something that actually looks from a different way. You have to understand the dataspace that you're dealing with, you have to observe what's going on, you have to know the enemy, you have to know those enemies, and we have to get business and enterprise to realise they're on a cyber battlefield.

[00:44:36]

Right, okay. And you're, to realise that's one thing and, you know, but to be able to achieve that transparency is obviously a huge challenge.

Chris: Yeah. Well, that's with us. Ironically, that's with us. So we achieve the transparency and the results of that transparency is intelligence leadership and actually intelligence direct to enterprise. So at the pace at which we see those preparations, planning, weapon development in the dark web, we're already putting that prevention into enterprise. And that's a big difference.

You started off by saying we don't know, you know, none of us can tell what on earth's going on in the dark web, you're saying well actually, we can now and we are beginning to do that.

Chris: We can, and that's the revelation, if you like, we can see that. We can see that. And…

But that's still, it doesn't solve the problem for businesses. I mean okay, so they know, you're saying well, they know where the enemy's coming from or what the enemy's doing, that will help them to prevent the enemy, but will it actually, that's a different thing isn't it, being able to stop it. You can't necessarily…

Chris: It is, it is. So you're absolutely right. So basically, again coming back to kind of a very simple example, in September 1944 the first V-2 rocket landed just down the road from me here in London and that rocket, it went into space, it came down very, very fast and the first we knew of that weapon's existence is when it put a crater in and killed twenty-four people. Yeah? It was a huge change. And right up until that point, that was actually a Zero Day weapon, yeah? And those weapons just don't appear, they are developed, they're honed and that version that landed here in September 1944 was called A4, and A4 had an upgraded guidance system from Siemens AG, for example, that that actually made it possible for that rocket to leave the atmosphere and come back, yeah?

Yeah.

Chris: And hit close to the target. So basically what we do is we break down, you know, we break down the methods of attack, we identify those, we identify where the adversaries break cover, so they break cover into the light web, you know, public-facing IP addresses, you know, they use certain types of weapons tactics, they'll use certain types of malware, and actually what we do is we immunise customers against those things as they develop at the pace that that Zero Day, you know, as I mentioned before, probably just under a thousand Zero Days that we saw in 2021, and almost forty-five per cent of those were subsequent malformations or developments on that weapon. So if you think about them, you know, if you think of 1944 V-2 weapon drops on London just down the road, had never been seen before, the world's shocked, everybody's looking at each other thinking where did that come from, that was A4 and then after that there were several different variants.

Yeah.

Chris: That did different things. And as Iain said, you add components, they add components. And they buy and sell and trade those weapons as if they were, you know, arms sales.

Iain: If I – I can see he's got you ahead a wee bit there, Jane, on the weapons – if I… A weapon in a cyber sense still has characteristics that break down into some key elements, let's just call them the detonator, the firing pin, the barrel, right, of a weapon. And what Jeremy Samide, our founder, has done is applied those military analyst tactics to identify those in the weapons before they've broken cover, before they're even, they may be targeting particular vendors, the vendors don't even know about them, and by knowing how they're constructed, he can basically immunise by making sure the equivalent of the firing pin doesn't work, you know, the barrel's twisted, the detonator doesn't work or whatever the weapon is, but in cyber terms it's called hash, you're on bad IP. These are the elements, then they don't work, they don't work. So they might land, but they don't go off.

Chris: Yeah.

[00:49:36]

And can you measure this? I mean can you actually show a return on investment?

Chris: Yes, absolutely.

Iain: You certainly can.

Chris: Yeah. I think we are the first organisation to actually demonstrate that quite clearly. Not only can we demonstrate a return on investment, we can demonstrate an uplift of efficiency in preventing you joining the victim pool for a cyber attack. So what we, we do something called 'mark to market' where we look at sixty to seventy different providers and we measure ourselves against them using clearing houses, or a clearing house to look at virus total, but basically we can measure it. It's the first time I've been able ever to be able to measure my effectiveness of getting my organisation off the Zero Day victim list and get them out of the pool for that, you know. But do that in a way that isn't scientific, you know, it's consumable by the executives who are going to be answerable for, you know, the resilience of their organisation, you know, in the new world. We're on our way, we're on a trajectory where enterprise is going to be forced, yeah, to play their role in terms of systemically important banks, for example, or internationally systemically important infrastructural banks, those kind of things. Critical national infrastructure, which is being redefined as we speak, about what is it. You know, protecting water safety dist… you know, reservoirs, distribution and so forth, all of those things. All of those things are now influenced by cyber. The method of control is information technology.

So who have you signed up, who's paying you to do this for them now?

Chris: So we obviously have our origins in law enforcement and defence, so we're still paid there, but organisations are recognising that they have to do something else, so we're picking up different organisations that are providing services. They would include vaulting companies, they would include…

Sorry, what companies?

Chris: Vaulting. So basically you collect information, yeah, so cyber vaults, yeah? So vaulting companies are buying us because obviously they want to protect against the evolution of weapons because they're being targeted very much because they're a great big honeypot of information that…

You mean like datacentres?

Chris: Datacentres, absolutely. Absolutely. And as people move to the cloud or they become hybrid organisations, those are the kinds of organisations that actually are starting to realise that their detect and respond stance, yeah, isn't working.

So there are lots of ways to crack a nut, as they say, and, you know, there's many, many companies out there in the world of cybersecurity attempting to do things in different ways, aren't there?

Chris: Yes, there are, yes.

Are you saying that yours is the only way to do this, or that you're the only people or are there competitors of yours that are taking a similar approach, what's the situation in the market generally?

Chris: So in the market, I'm going to make a statement that we are the only organisation doing what we do, because what we have has been developed from the original cyberwarfare programs in the US, it is a platform that has been machine learning and refining that intelligence aided by cyberwarfare analyst experts, those people briefing the world on what this, on what the dark web is and what's going on in the dark web, those are the people we've hired. For eight years that's been, their tradecraft and their capabilities have been embedded in our machine learning platform called Zero Day Live. So Zero Day Live looks at, you know, looks out in an observatory to see what's going on, the development of the weapons, we take the weapons, we deconstruct them, we create indicators of compromise. So basically what happens, Jane, is each of these weapons has a signature, yeah? And we obtain

the signature and we inject that, we inject that into security architectures before that weapon is weaponised against you. We also do some other things, which is we sense the changes in the way that forward operating bases are created, infrastructure's created, and we also send that information, you know, those intentional assets, if you like, that are being used as part of the attack alongside the weapon. Or to introduce the weapon more effectively. So we do all that. [00:55:15] Not only do we do that, we create a single pane of glass through which you can observe that and you can question that in English language – I'll come on to that in a moment – but also we send that protective data elements, you know, those individual pieces of cyber DNA that are injected into your firewalls, your end point protections, your security, SIM, information management systems. Your cloud compute, architectural firewalls, all of that we send, and it is precision. Yeah? It's precision, high comfort and it's at the grade that is keeping the world safe at the moment, cyberwarfare, but it's at that grade.

So, right. Right, so well, just, you know, there's obviously masses of companies out there that have worked on cybersecurity for years, I'm thinking of companies like Symantec, Cisco and more recently, the high-flying unicorns like Darktrace, for example, and lots of other start-ups looking at, you know, the whole area of cybersecurity. I mean are you saying what they're all doing is wrong and what you're doing is right, or…

Chris: No, we're not actually. We're not actually saying what they're doing is wrong. What we are saying though is that all of those companies you mention, Darktrace, you know, Cisco, Symantec, you know, obviously one of the big unicorns, CrowdStrike, yeah? They're only as effective as the cyber intelligence they use and consume. So we can measure an uplift on Cisco, CrowdStrike, you know, Microsoft, Darktrace, we can measure the uptick in performance. Many of them, you know, many of them are sharing and buying and trading different types of intelligence, oftentimes that job of managing that threat intelligence to actually get the effect of prevention, as opposed to detect and respond, is expensive in people and money. And it doesn't work, because what we've seen is, a huge, a huge uptick of, you know, uptick in victims over the past number of years. So what we're not saying that these guys are wrong, we're just saying that they may need to consume our intelligence to

perform better. And that is the return on investment upgrade that we think that enterprise needs.

So shouldn't your, your technology is so fundamental evidently then to global security on the internet, shouldn't it be something that governments and enforcement, you know, the security enforcement agencies should be sort of running and making available, making available to everyone in a way so that we can all be protected.

Chris: You know, in a way, possibly. But what we're doing is making our technology available to defence and law enforcement so that they can actually get to the job of defence and law enforcement. We need to defend them first, because actually they are also victims and targets for the attacks that are being launched out of the dark space. So disabling law enforcement and disabling governments is, you know, is a nation state, you know, I wouldn't say an epidemic, but it's definitely something that they do. So protect those guys first, because in effect that's what we need to do. And also remember that most of those governments do have cyber war fighting capabilities. So they actually also want that intelligence, yeah, to protect themselves. So… and yeah, we're a private enterprise, we're not in it for fun. Yeah, so we're in it to create a, say, a billion dollar start-up company, which I think we will achieve, and that's my aim for the company. And also, you know, we are, we will only work with those organisations that are within NATO, so friendlies. And in effect, the enterprise is a very, very distributed, it's not what it used to be, so it's hybrid, you know, it incorporates, you know, web-based Compute, it's offloading and outsourcing to service providers, and including out loading workload like Compute to Amazon, for example. So, but the responsibility and the accountability for the resilience of an organisation rests fairly and squarely with the board of the commercial enterprise. And it's those people that need to buy us to protect them.

[01:00:51]

Well, it sounds like you've got a bit of a killer weapon there, or, you know, if you've got the next generation of protection on the internet, then that's sort of a bit of a silver bullet, isn't it? I mean that's going to be…

Chris: You know, nothing is a silver bullet in the world, because you don't know how the world changes. You know, Eddie Obeng, who kind of is also a good friend of mine and also taught, you know, he taught me two things. One is, never ever place or misplace concreteness, yeah? Because you don't know what changed at midnight. He calls it the world after midnight. So if you look at it, you know, his perspective is, the world did change last night at midnight, and it always changes every day at midnight. And I think it's a great piece of philosophy to look at the way that Zero Day Live works, yeah? So we know the world changes every day at midnight, we know that the dark web changes and the light web changes, technology changes, business changes, all kinds of things change, yeah, at midnight. So basically, what we've developed is something that actually works consistently, close to that, very close to that particular clock speed. And one of the issues obviously that stems from being able to have an internet that works at light speed also means that crime happens at light speed, yeah? And particularly…

Iain: Jane, there's a lot in cyberspace who make bold claims, I think the thing, one thing where we are is we do make bold claims, but we can back up what we say, our effectiveness in actual support of security decisions made, if you like. So all the brands you mentioned, right, is that we can uplift on their cybersecurity because we're looking in a different direction. We're looking towards the adversary. We can evidence notable attacks over the last two years, we can go through and do the anatomy of those and we, our clients, we are protected against the viruses that hit others. You know, LockBit 2.0 is a notable example of autumn last year which hit a number of organisations quite significantly. We could show the anatomy of the evolution of that weapon where our customers were protected against that weapon, because at the time of the evolution in the June, July and the August where these really got nasty and stealer components were added, we were the only company in the world that was looking at them. And the thing about the weapons is that when they become really potent they are used within two to three weeks, so the timing of uses is so critical and the timing of being able to provide immunisation is so critical. And so, you know, clearly we will promote what we're doing, but actually Chris and I thought very long about what we did next and we were drawn to the Blackwired proposition, because frankly, it's the first time since my days in the army, I feel I'm in a noble space. People and businesses and communities and governments are getting crushed.

When this, when we went through the story with the founder about what he was looking to do and what he'd achieved in law enforcement and government, that's what drew us to get involved. This is something that's applicable everywhere. Chris talked to vaulting, but you know, banking, healthcare, aviation, insurance, it's applicable everywhere. So of course we're going to speak strongly about how much we believe in it, but everything we say we can measure, and that's the difference and that's what's just recently – and Chris, you're going to shout me down – but, you know, we've just been put forward by the DCMS, the government body, for the innovation award this year. You know, we're in the space and these guys really know what they're talking about in their assessment, you know. So…

[01:05:05]

Chris: Yeah, that's it.

Iain: … super-competitive space, but really, really we feel…

Yeah. So are you, these techniques that you've developed, are you saying they couldn't really have been developed by anyone else out there in the market? Have you got…

Iain: They couldn't be copied, they cannot be copied readily because of what Chris is saying, is these are eight years in the making. The algorithms that form the basis of what we do is representative of how military analysts would operate and they've been built up and enhanced and enhanced and enhanced over the eight years to get to this point to bring it into the enterprise sector, and it's so strong. And intelligence is perishable, so you can take the intelligence one day but it's no use three weeks later, particularly in that cycle. So the work that we have done would take years to replicate, is our strong belief, and that is what we're hearing also from the marketplace.

Chris: Yeah.

Okay. Won't the hackers, by definition, always be one step ahead?

Chris: By definition, weapons always defeat defence, yeah? But if you start with the weapons, as we do, that one step becomes maybe half a step.

Iain: We both study military, we both study military, and this is getting behind enemy lines, is finding out what they're doing, is watching what they're doing. Some of the access has taken years to achieve in its own right, to be listened to the chatter of what is being discussed next, you know. And if you think military you can really think of your [incomp] strolling in the Western Desert [incomp], you know, thinking differently, get behind enemy lines, disrupt. And that's what, that's what this is doing in cyber terms, is getting in behind, finding out what's going on with a very, very different lens.

Chris: Yeah.

Military strategists thought that, almost universally thought that Russia would succeed in conquering Ukraine in three days. I mean they were completely wrong.

Chris: They did, but how much intelligence did they have about what was going on and how much intelligence was released to folks. So we have no transparency on that intelligence, Jane, at all. We don't know, I can't confirm it, we don't know. All we know is what we see and what we can see is that preparations for that were happening, with false flag operations against NATO and our forces, were happening months before, yeah?

Yeah, so they were right about the invasion but they were completely wrong about the impact?

Chris: Well, yeah but…

I'm wondering whether that has parallels in your world as well?

Chris: I would not want to, you know, yeah, our CEO and others may be able to comment on that directly, but I wouldn't want to comment on that, really. But what I

would do is give you another example, Jane, of what's happened because of my experience in financial services, so the European banking association, the British bank association said that banks needed to operate multi-factor authentication, yeah? Because that was a way of actually almost eliminating, you know, fraudulent use for online access from mobile phones, etc, etc. Actually, we see that a number of weapons have been produced that defeat multi-factor authentication, and you've just seen an example of that in terms of Okta, which is obviously one of the biggest multi-factor authentication providers, service providers on the planet, right? So what we see is, that development happened in real time, yeah, and then we set up a defence for that into our organisation. So that's an evolution. There's another evolution around Zero Trust, everybody talks about Zero Trust but they don't understand it. You know, I have patented data center technology in Zero Trust. They don't really understand what that is and unfortunately Zero Trust authentication and authorisation is also compromised, you know, severely compromised. I'm not saying that to be scary in any way, but you have to listen to what's going on, you have to have observation on what's going on to see how your next, your future is already being compromised by folks whose only job it is, is to attack you, yeah? They're not supporting, you know, a business, they're not supporting a balance sheet, they're not supporting shareholders, all they're doing is building and spending twenty-four hours a day, 365 days a year working out how to attack you, attacking you and getting that job done. So that's the real difference. [01:10:29] Some might say, and I did mention to the former director of the NSA that we work with, I said this is, this is asymmetric warfare, yeah? You know, guerrilla warfare against the enterprise. Asymmetric being a small force with knowledge superiority, weapons and tactics superiority, you know, attacking a bigger enemy and being successful at it. So it really is that case. So you have to decide whether or not you're going to persist with detect and respond, because it's very, very wasteful and it's unsupportable going forward, or you're going to screen as much of those attacks out, yeah, using our kind of technology. But you can also use our technology, incidentally it's being used also in the recovery phase where somebody has also been cyber attacked, because, you know, the same information, the same data that we send to them for defence can also be used in dark trace and so forth to illuminate where fragments, if you like, of the weaponry, the malware and so forth, are hiding in the client's estate. Because we also see that once you've been cyber attacked, you're highly likely to be cyber attacked again.

Yeah. What about, yes, I realise we're coming to the end of our time, so perhaps just a final question. Would you, could you look into your crystal ball and maybe give a bit of a forecast as to how you see all this developing in the next five to ten years?

Chris: Yes. So the crystal ball would be, you know, the key things are transparency and oversight on two particular areas. One being cyber and the other one being crypto. They are the two most significant problems in the world today, because we have no oversight, yeah, no transparency on those areas to speak of, but also we have no means to, no means to control them, no means to apply enforcement and we don't have effective standards in place. And even if we did, we couldn't enforce them. So what I can see in my crystal ball is that there will be investment in two things: there will be investment in being able to achieve transparency in those two environments from which regulation will be developed; and the regulation and compliance and enforcement will be in flow of transactions as opposed to bolted on the side, yeah? So I think that that's, you know, that would be my prediction for the next five years and we hope that we're going to be providing the mechanisms by which we make good regulation, good enforcement, and we also make great decisions that help everybody, based on the dataspheres that we have oversight of in both those areas, which is crypto and – sorry – which is cyber and crypto.

Well, thank you very much, Chris and Iain. I think that's all we have time for now, but it's been a fascinating discussion and I look forward to seeing the progress of your organisation, of Blackwired, and how these things do pan out, and hopefully you will continue to be able to put these measures in place which will protect us all from what could otherwise be a very disturbing situation.

Chris: Ah, absolutely. And I'd love to continue to obviously contribute to the Information Technologists Livery Company and also to, you know, to get these kind of stories covered now, you know, because they are important.

They are, very much so, yeah. Thank you very much indeed for your time.

Chris: Ah, thank you Jane.

Good to meet you.

Chris: Yeah, good to meet you, Jane.

Iain: You too, bye.

Alright. Bye bye then.

Chris: Goodbye.

[01:14:45 end of recording]