CR115

Power of data in complex industries with Chris Carter, BAE Systems

Capgemini

CR115

Power of data in complex industries with Chris Carter, BAE Systems

Disclaimer: Please be aware that this transcript from the Cloud Realities podcast has been automatically generated, so errors may occur.

[00:00:00] Be honest. It's gotta be a boring Sunday afternoon. If you're on eBay looking for de amongst, I dunno. That's a very part, a very part.

Welcome to Cloud Realities and original podcast from Capgemini. And this week a conversation show about modern day intelligence and the increasing complexity of the associated cyber considerations. I'm Dave Chapman, [00:00:30] I'm Esmee van de Giessen and I'm Rob Kernahan and I'm delighted today. Joining us for this conversation is Chris Carter, who's the director of Key Accounts and Australia at BAE Systems.

Hey Chris. Hello. Great to be here. How are you? I'm very good, thanks. Very good. You, your namesake is the guy that made the XFiles. I've just realized that It is. And also a very successful author. Right. You're in good company. Very good company. I mean, that is No, but that's, uh, you got X-Files and, uh, murder novels.Yep. I [00:01:00] mean that's like, that's quite a dark. Heritage to the name, isn't it?

I see there's a link there. Like the X-Files though. Oh, ACE. I, I, I'm sort of considering a, a rewatch of the XI haven't seen the X files since it finished. Now, do you think though, that would become horribly dated? I mean, you know, Jillian Anderson, David de Coveney, brilliant chemistry on, uh, on screen, great sort of writing, buti s it one of those 90 shows when you go back to, you go, I regret rewatching this. So I think I have two I two potential issues with it. I have actually thought about this on the two [00:01:30] potential issues that I think are one, it went off the boil anyway. Yeah, right. So after about season five or six or whatever it was when, especially when Mold and Scully weren in it, like you do, ask what the point was of continuing the Xbox.

Well, it was the chemistry that was literally the show, wasn't it? That is the show. Yeah. But then the other thing is. Modern TV isn't like 23 episodes a season for nine seasons, is it? So just sheer volume means you're gonna have some chaff in there. So now you got, I think you gotta go eyes wide open. I reckon [00:02:00] it's like I always wanted to rewatch Twin Peaks, but I think, oh, no, no, I have done that. Now you go back. Is it, is it as good? Uh, twin Peaks is, uh, maybe even better, I think now. Is it? Especially since the return. Have you seen this the third season?

No, I am. You haven't seen Twin Peaks, my friends. Are you taking a story than just like, munge? It's like lost it. Lost its way. Oh, twin Peaks is a wholly different cut of fish. Have you seen Twin Peaks? Chris? I have not seen Twin Peaks. Have you seen Twin Peaks? No, I don't think it's another David Deveney special. Is it David Ov and Twins Peaks? No, it's, uh, no, it's, um, McLaughlin.

That's it. [00:02:30] Karl McLachlan. That's it. Sorry. I think there's a whole, I think there's, I think, I think you as a podcast two need homework. You your homework to start working your way through Twin Peaks. You came the building the show, so now you've got to do homework. I, all I can keep thinking about is, is, uh, Peaky Blinders.That's the only image I have in my head, but that's. Probably far away from, it's quite D and Thomas. Shelby. Oh, is that because the peak thing? Yeah. Yeah. No, super different. Yeah. Okay. Super. Very, I mean, it's like opposite ends of the TV spectrum. It happens in my head all the [00:03:00] time. As if that wasn't confusing enough.

Robert? Well, speaking of tv. Yeah. Black Mirror, Charlie Brooker. Did you see the latest season get through the mob? No, that's not about mirrors. No it's not. Just to be clear, is it blackmail clear there? There's an episode where they install some software in the lady's head and then you know, they start playing adverts and all that sort of stuff and go through absolutely it. Excellent episode. Yeah, but it led to a confusion, which was lots of untapped potential in the human brain. Yes. And we aga before we go on, Chris, have you seen that

[00:03:30] episode of Black Mirror? I haven't seen that episode. I have seen Black Mirror. So just so you can, just so you can, I mean, we all struggle to keep up with Rob's confusion, but just, just to give you a fighting chance.Okay. So in the, in the episode, uh, and no spoilers for those who haven't seen it, but broadly the setup is a woman kind of has a brain aneurysm or something like that, and they can treat that by putting like a chip in her head. And they do that and it's like a medical miracle and everyone's delighted.

But then the company starts to monetize the [00:04:00] chip and starts to, if you want to use that it like on a free or freemium, you would then get ads that came into like you, so you, so you would, in the middle of it, you'd be like, Hey, have you ever used, you know, the Apple iPhone? They'd be like that. So that's the setup of the show. So on that, Rob, go. Okay, thanks for that context, Dave. Yeah,

I'm here for Rob. So. Lots of, uh, actual science going into the human brain interface. And if you were offered the opportunity to rent your capacity [00:04:30] in your brain for compute power Yes. Like ultimate distributed cloud. Yeah. Yeah. And you plug in.Would you do it? Absolutely not. Under no ircumstances, that seems completely open to abuse.

But if it's all safe and secure and they're just using the bit of your brain, well that's what the, that's what they bought into on the show. So I know if you're opening with Black Mirror, you telegraphed your answer because what I'd love to do is install like a Legacy's 90 ERP system in your head cause that would be the ultimate irony with you. It would [00:05:00] be, it would be being in hell. It'd be like being trapped in hell. You know, if like, you know, 500 pounds. A week's worth of compute, 500 pounds, I dunno, whatever the number would be. What would you go for for me to install a legacy CRP system in your brain?

What's your price point? What's the price point? I want a week's worth of compute, a week for a week's worth of computer, for a week's worth of compute for a, you know, an enterprise. What you gonna charge me?

I And is this likely to be like just a one week one off or is it an ongoing Well your brain's like a [00:05:30] subscription.

They can turn it on and off when they want. Yeah, yeah, yeah. So when it popped off, so you know, when you watch that crap TV, uh, under deck or whatever it is about the stuff you look that below deck deck, you loves this guilty pressure.

So you watching that, the tv, that is what I am. And you, and you don't need much processing power to watch it. Yeah, yeah. It's all wasted. Rent it out. Uh, it would cost a a lot of money. I, I'm thinking along six yourself outta market, six digits, 60. You price yourself outta the market, aren't you? And then not only that, and then an unlimited level of insurance around them abusing the situation.[00:06:00] Yeah, I, I, yeah, they're not, they're not gonna buy that. Well, I, I, I'm okay with it. I'm okay pricing myself out of it. So, because that, I, I would not be an early adopter of this technology, but if you think about it, easy access to money and you do it, is it then something that people would do and that's the bit I'm confused about?

Or would the morality of it go? I, I actually do think. If you could, they probably would, wouldn't they? Yeah. I, I do think people would not consider the security ramifications or, you know, whatever it might be. 'cause [00:06:30] they would be horrendous.

The whole, the whole theory of you come to work and you plug in and defeat the language interface, the keyboard, the mouse, and you're directly communicating with it.That, that is ongoing as a scientific sort of Yeah, yeah, yeah, yeah. Research. So when we get there, then how'd you do, how'd you do it? All An element of- I mean, I'm not even, I've gotta say I'm not even thrilled about the idea of just even a chip to remote control my computer. I don't, I don't love the idea of, I have to say, but actually renting out my processing capacity, you

know?[00:07:00]

Bet you 15 years that's up on the coast. I, I'm not doubt it might happen. Anyway, that now that is a future reality right there. It's that. Well, that's the confusion, isn't it? We have to wait. We'll come back to that in 600 episodes of time. On that note, Chris, thank you so much again for joining us today.

Let's start with understanding a little bit about the world of digital intelligence specifically. What does that mean within the context that you work in?

Sure. So people will often be familiar with. Uh, BAE [00:07:30] systems as a provider of, uh, large platforms, ships, aircraft, armored vehicles. But, uh, increasingly the important thing is less the platform itself, but it's the data, right?

That it can collect. How that platform is then connected to and integrated with other systems and the decisions that can then be made, uh, with that data. So my part of the group is really all about. The [00:08:00] integration of data from multiple platforms and capabilities, ensuring that that is secure, uh, against adversaries mm-hmm.

And ensuring that better decisions. Can be made more effectively, whether that's by the military, but also by law enforcement and security agencies in that broader context of national resilience as well as just defense. And

it must be quite chaotic 'cause data is coming from literally everywhere, isn't it?

You've got all these platforms, there's loads, there's just stuff out there collecting it all [00:08:30] sort, sort of the scale and the size. It, it must be quite a challenge to just be able to find the bit that you're interested in. And go there. And I suppose that's the first big thing, isn't it? About normally when people think about data, it's more static than what you deal with.

This is like high velocity stuff. So it's like, uh, and then just the sheer, what do I process? How do I disseminate the information and set, send it on it. It is like, it is really complex challenges you face it absolutely. [00:09:00] The challenge will be very different depending on the, the nature of the particular mission.

So you could look at something like missile defense. You have to be able to make a decision. Is this a threat within the space of seconds to be able to achieve a, a countermeasure against, uh, against that? Yeah. But in other, it might be maybe with law enforcement worrying about how do you appropriately and securely retain.

Uh, evidential data, right? [00:09:30] That might have to last for decades because it's been used to secure a conviction, uh, in court. So there's a huge variety there. But certainly thinking about the aspects which are perhaps not unique to defense and security, but which are particularly acute challenges, uh, is what we spend a lot of our time doing.

Perhaps before we go into that in a bit more detail, maybe just take us through what the last 20 or so years of evolution in this space. As look like for you. Um, I understand you're in a smaller organization to start with [00:10:00] that was cyber centric. Yep. So maybe take us on your journey. Yeah. So I've been with the company for 17 years.Mm. And I started in what was at the time a medium sized consultancy focused on. Data, data analytics and what's now called cybersecurity are they often was called information assurance at, at the time. Mm-hmm.

Oh, I remember those days. Information assurance. Yeah. They were innocent. More innocent indeed.Yeah. When the threats weren't quite as sizeable as they are [00:10:30] today. And the work that we did initially was sometimes seen as being a bit peripheral. Mm. So the, the important thing was the big platform. It was the aircraft or the, or the ship. The huge

transformation over that time is that data and intelligence has become central, right.

Not peripheral. And we see that when we're at major events. It's one of the things I was reflecting on. We used to be the little stand in the corner. Yeah. Nobody quite understood [00:11:00] what we did over there. Security state in the corner. Yeah. Not security. Where are they? Over there? Yeah. Yeah.

But we're now positioned really centrally because it's about how do we pull together?Uh, and integrate that data from across the different domains.

So this presumably is certainly about the, I would imagine, evolution of technology over that period. Mm-hmm. But it's also, it's the abuse of technology, isn't it? And the use of technology in nefarious ways that must have driven that change in importance.[00:11:30] Yeah, and I think as we see the adoption of new technology, it will always be, uh. Utilized in ways other than its mate is intended. It was the first thing with ai. AI is cool and then the hackers started going, AI is cool. You're right for exactly the reverse. Or wasn't it? It was a sort of, it didn't take long.

No. Uh, and so there's a, uh, a constant process there of adapting, understanding for our customers [00:12:00] simultaneously. What are the threats that this new technology poses be that. AI enabling misinformation, but also what are the opportunities for our mission? So AI can simultaneously enable misinformation at huge scale whilst also enabling an organization to conduct open source intelligence operations to identify and respond to that misinformation much more effectively than you ever could just with human analysts.

Right, right. And the, the change in nature of all of that, for all of various different reasons, we've just, we've just alluded to. Has led to, [00:12:30] presumably that's what what's got us to concepts like MDI or I believe it is multi-domain integration. So just wanna sort of set out what that, what that means in sort of terms for the listener who might not have heard of such a thing.

Sure. So multi-domain integration is a term that's used for integration of the different operational domains. In in a defense context. So the word domain is, we might come back to, is quite overloaded with different meanings. Yeah. In this context, air C, land space, cyber, sometimes are [00:13:00] they a bit disputed?

Whether that counts as a separate domain by some people, but the multi-domain integration point is therefore about the fact that the threats that you are trying to counter are not gonna be limited to one specific to one of those mates. Yeah. Yeah. So. You take, say, space, for example, as an operational domain.

It's also enabling connectivity for ships, soldiers, vehicles, aircraft. [00:13:30] Uh, it's enabling sensing. And another huge transformation, of course, has been the proliferation of space-based capability and what that means in terms of data and the coverage of data globally. So you can no longer think if you are a, developing a new defense capability about just a particular platform and the systems on that platform.

Mm-hmm. You have to think about how is this gonna be integrated with everything else in, across those different domains in the, in the battle space. [00:14:00] But I think importantly, and, and, uh, you also have to think about the fact that you won't necessarily have. Connectivity right across those domains. Right? So it's really important to achieve that integration.

But you need to be very conscious when you're deploying new technology that uh, the links you have to other assets could be denied, degraded, could be low bandwidth, could be very high latency, and as one of the [00:14:30] particular complexities that we would face. It's

when you take a technology that's been developed for.

Uh, that similar kind of data integration in perhaps a, a commercial context. Yeah. We've got so used to abstracting away from where's the compute located? The actual use, yeah, yeah, yeah. That I'm running this, this workload on. Yeah. And that's the great thing about, about cloud. You don't need to worry about that.

Yeah. Well if you are sitting at the end of a radio frequency data link on an island [00:15:00] somewhere and you have an enemy conducting, jamming against you. Then you really, really do need to care about right where that compute is, where the workload is running. Yeah. And what are the implications and is that causing a, a proliferation of edge.

So you've got enough near you so that when that does happen, I can still maintain, you know, the ability to compute stuff. 'cause that we, we normally think about cloud as being, we're gonna centralize, but now actually there's this compute every everywhere type thing. Is that, and, and the sort of like you [00:15:30] take your compute with you as you go.

That's one key aspect of it. Certainly it's the ability to do that sort of processing. At the edge. Um, again, space is an interesting example here. Often the constraint with sensing from space is not how much data you can collect, it's the bandwidth you've got to send it, transmit that back to the ground when you're passing over a ground station.

So thinking about how you can use things like, uh, AI at the edge to identify what is the data that is gonna be of most [00:16:00] interest to the commander on the ground, and then transmitting only that information directly to that commander. Becomes transformational.

That has a huge difference when you're talking about quality versus quantity.Mm-hmm. If you have AI help, you decide, okay, we, we need this data. Instead of, oh, let's just pull it all in and then we'll see, you know, what we can make out of it.

Well, we often talk about sending data from the edge can be very expensive. Sending it from space is even more expensive. So you sort like this and make sure it's right and send just, yeah.[00:16:30]

What you need, isn't it? It's the, uh, be a bit sharper about how you think about it, but does it mean that you really know that you have high quality data? 'cause I think in the world of data, it's always been up till now. It's the discussion. Yeah. But the, the quality of the data is like we need to start there first.

Data quality. Yeah, absolutely. Really important. But you have the extra challenge in, in many of the operations that we support, that the data might be poor quality, not just because. It's inherently technical, [00:17:00] challenging problem, but because somebody is deliberately hiding or obfuscating what they're doing mm-hmm.

Running a deception, operational, running a false flag operation to make you think that something else is happening. Right. So the level of, uh, assurance and trust that you can have over the data. Certainly when you're making decisions about perhaps, you know, to arrest somebody or to. Conducts our military operation becomes, uh, hugely important.

We, we often have a chap on the show called Dave Snowden Effing [00:17:30] Framework. He talks about the corruption of mass open data sets as well, where people very subtly change it. That then forces the systems to maybe act or decide a different way. You got a viewpoint on that if it's becoming quite prolific.

'cause you know, if you take, there's lots of use in open data, but if you know it's bad, then well, how do you tell it's bad? I suppose it's

a sort of. There's potentially quite a lot of concerns around that, I think, and, and in also in, in

terms of when that data is then being used as training data. Yeah.

Mm-hmm. [00:18:00] That's right. For AI models. Exactly. That. And I know you've been talking about sovereign ai Yeah. You know, on the podcast and what does that really mean? Yeah. You have to have some real concern about could, are there attack po and channels for, uh, somebody to, it, it feels like it does open up a number of surfaces that perhaps didn't exist before.

Yeah. And the non-deterministic. Nature of the behavior, which has some big advantages in terms of capability you can deliver. Yeah. Yeah. Just makes the problem for a, [00:18:30] uh, somebody who's focused on security in a, in a, let's say a government role. Who, who's responsible for accrediting a system or how do you assure, or a credit the behavior of a system that is inherently non-deterministic, right?

That rubs up against policy problems that are. Very, very difficult.

Well, you got that thing where you go, you've trained it, and then you ask it a question. It does one thing. You do it again. It does something else. It does something else. You can never actually be sure which way it's going to go, and especially in this context, that can be quite, there's loads of [00:19:00] advantage out there, but it's just the, how do you trust it?

I suppose it comes down to that. How can I assure that this is gonna do the right thing when it's needed, when it's like you say time critical. Hmm. One of the things while we're in this cyber domain that I wanted to touch on and just get your perspective on is let's say over the last 20 years, to your point earlier, actually stepping back from that, to your point earlier you said that there are known domains and then sometimes there's cyber as well, and that's in debate in some way.[00:19:30] Why is that in debate when, when you actually look at, you know, what's been going on over the last 20 years in the world of cyber? Mm-hmm. It is quite clear that there are, there's a, it is, there is a lot of activity there. Yep. But what's your perspective on why we are where we are and you know, what do we do?So I think everyone now agrees thatcyber is an important domain in the sense that operations that are conducted. The cyber [00:20:00] domain defensively and offensively. Yeah. Have huge implications. Yeah,

yeah, absolutely. What I think is in dispute, if you like, is, is it the right answer to consider cyber as a separate domain to the others? Given they are so tightly, yeah.It has to permeate through, doesn't it? As a concept, because I think the concern is if you treat cyber as a separate domain, you run the risk of creating another operational silo. Yeah. [00:20:30] Silos away. Yes, I get you. Yeah, yeah, yeah, yeah. So at the moment, does it, is it literally drawn as like a horizontal across the others?

If you were to do a basic whiteboard diagram of that. It is often depicted in that way. Yeah, that that's the classic security. When everybody draws the diagram and security says, where's security? And then somebody said, we'll just stick it as a horizontal down down the side. Isn't this the classic sort of, how do you respond to that as given we're not on film, as Rob said?As, as Rob said, I a vertical line. I mean that's the kind of [00:21:00] misinformation watch out for him. Yeah. Well, yeah. They've kind of confuse us all with that. The world of cyber then, from your perspective? So when you look at cyber, just through a commercial lens of, of any big commercial organization, yeah. It has gone from actually to use what you were saying earlier, from information insurance, like just another role in the IT department.

Mm-hmm. And maybe with a bit of audit or something. Two, you know, either enormous services that organizations buy in or [00:21:30] minimum you have to set up your own control centers and it's a very, very sophisticated operation today. Like you, you're dealing with business risk, you're dealing with tech, very cutting edge technology a lot of the time, and

enormous complexities of data.

Yep. Do you see that any different in the space that you are working in or are the parallels quite. Similar. I would say it's that, but even more so. Right? Yeah. Yeah. If you are a company, it's clearly important to have that [00:22:00] protection in place. Mm-hmm. But there's a business risk versus investment decision about how much protection is it reasonable to be in place?

Yes. Right. Are we compliant with regulation? That would usually be important. Yeah. Are we. More protected than our peers in this sector, such that a criminal group is probably gonna go after them rather than us. That might be the way you frame the problem. Yes, yes, yes, yes, yes. But if you are a, a government, so it's not that you've got no risk, it's just that you've got less risk than your competitor or your neighbor.Yeah. And, [00:22:30] and we see that criminals will tend to target. Weaker, uh, don't be the gazelle at the back. Absolutely. Yeah. Yeah. It's that,

it's that classic joke where the, the two guys see the lion coming at them, and one starts to put their trainers on, and the other one says, well, you're never outrun a lion.He goes, I don't have to outrun the lion, I just have to outrun you. Yeah. That's a security paradigm, isn't it? But if you are a government or a military organization, then you have to know that there are [00:23:00] hostile actors who will commit. Huge resources specifically to target you regardless of how Yeah. Hard you've worked and how much investment you've put in.

So what we see is as different is that there are certain capabilities, types of hardware or software solutions, which don't really make economic sense for a company. Yeah. But which. [00:23:30] Necessary if you're protecting secret or top secret information. I hear you. I hear you. So things like disconnected cloud environments.

Mm. I would say, well that doesn't, that defeat the whole point of having a cloud environment. The fact that you're disconnecting it. There's a different, uh, balance of risk versus cost you might apply. Right. And one of the other areas that we work in, which I think is a illustrative example, is something called cross domain solutions.

Uh, this is importantly and to add to your, I think you have the point of the podcast around things which can be confusing. [00:24:00] Mm-hmm. Mm-hmm. The word domain there means something different from multi-domain integration, right. So, right. So we're talking here about domains of trust or domains of classification.

So more similar to perhaps a network domain in an it Yeah. Context. And so a cross domain solution is a capability that allows you to transfer data between perhaps a secret network and an unclassified network.

But you get, you get, and you see in the industry, if you take a heartbeat of the industry three years ago and compare it to where it's today, the, uh, cloud service providers are investing [00:24:30] huge amounts of money in exactly what you're talking about.

So air gap solutions, you know, your own dedicated region, and we see that rising fast, especially when you use the sovereign word that's a. That's part of the conversation. So yeah, you're absolutely right. Five years ago, let's not have this conversation. It's not the point of cloud now that fragmentation is occurring.

'cause it's at the top of everybody's mind about exactly the things you are about how you protect

yourself. Yeah, absolutely. You are right that those kind of disconnected cloud environments, sovereign [00:25:00] capabilities have become increasingly important. Yeah. And it drives requirements for a different set of solutions than you'd really need.Anywhere else,

right? ‘cause what you would say, it’s a disconnected cloud actually. It can’t be completely disconnected. You still need to be able to, you have to update it. It’s a cd. You can come in with a CD and plug it in. It’s like, you know, the 1980s, I would say some of the last uses of floppy discs, uh, anywhere still out there is for, has been at least in the past for those kinds of. Data [00:25:30] transfer across, I bet, you know, classification boundaries.

There’s an alarming amount of aircraft that still use Floppiness to update their navigation software. I’m still astounded to this day that it’s not a USB key, but it’s still a floppy. They still make ‘em, yep. Still exist.

No, you sketch the picture.I think of not only highly complex environments dealing with very sensitive. Highly security sensitive issues, but also acting on often on the cutting edge of technology because the people that you are kind of protecting against [00:26:00] are also on the cutting edge of technology. How on earth are you finding the right level of skills and capability to, to maintain what I’m sure are pretty massive operations?

So as with many other sectors, attracting and retaining. Yeah, it’s difficult anyway. Yeah. The advantage that we have in, in this sector is that sense of mission and purpose. Yeah. And I would say for the majority of our people, that’s, that’s the motivation. Right. It’s feeling that you’re working on an [00:26:30] interesting technical problem.

Yeah. But the reason that you’re working on that problem is ul ultimately protecting your, uh, your nation, your, your family from, uh, from threats.

Is that also your drive? Yes. It’s the base of intrinsic motivation, isn’t it? Purpose, then you’ve got mastery, then you’ve got autonomy. But without the purpose, it’s difficult to motivate, isn’t it?So it’s a, yeah. Yes. And I thought about that from time to time. What would my job be if I worked in a [00:27:00] different sector? Well, probably 80% of it still gonna be looking at financial spreadsheets or having meetings with people. But that underlying driver of the reason that we’re doing this is, why are we here?Yeah, yeah, yeah. Why are we here? Yeah, often thought about what I’d do if I wasn’t in this job and I’d like to say I’d perfect the, uh, line joint fries with that. I actually think you’d be really good at it. Do you think so? Big smile, overenthusiasm Overenthusiastic burger seller. Excellent. Yeah, you’d be great at [00:27:30] it.Is it, but the, the other thing that occurs to me in terms of the complexity of environment you’ve just described is the levels of partnership that must be going on between different organizations. A level of urgency in those partnerships, I’m sure an increasing level of digital collaboration. Mm-hmm.How is all of that developing over time? Yeah, so that’s, I think another thing that’s changed a lot really in the past, sort of five years, five to 10 years, has been increasing importance of [00:28:00] partnership and collaboration, but also a proliferation of new partnerships. We see, for example, Orca as a partnership between three nations that are within the.

Five Eyes. That itself is an important partnership. The us, Canada, uh, uk, Australia, and New Zealand. It’s no longer just about from a defense perspective, nato. Mm-hmm. As. See a longstanding, you know, partnership organization, uh, in Europe and the North Atlantic. There’s the term mini [00:28:30] lateralism is sometimes used in international relations.

So there’s, you know, bigger than bilateral, but smaller than multilateral. There’s a, there’s a whole middle level. How did you ever know? Yeah, I did know, know, 3, 4, 5 partners working together on a particular topic, a particular operation. And that’s a trend in geopolitics to do with, you know, the alignment of.Nation states, but it flows through into technology because it means if you’re going to work out how to collaborate and communicate, you need to have an approach that’s flexible enough to work with those [00:29:00] different contexts.

You sort of being, you’re coming from a world where it’s sort of like, it’s my nation state,

and now you're working with these.Multi-nation state, that's gotta take a while to get the trust in and the ways of working aligned and everything else. How, how do you find that from a, a cultural alignment perspective? I mean, you're just integrating data sets with different taxonomy. That's gotta be a nightmare on itself. But then just everybody's trusting everybody to be able to share in that way.

That takes years. I, I, I would've thought, what's your view on that? Trust is absolutely the, the underpinning to a successful [00:29:30] collaboration or transformation there. And, and you have to focus on building that. Hmm. I think starting with just avoiding. Misunderstanding and miscommunication. I mean, just some of the words that we use, but even by the time you've got into the same language, the words that we use are, you know, not the precise precision of those meanings can vary.So I mean, one memorable example where a customer handed us a document that was labeled secret. Mm-hmm. This is an international customer and our security team therefore thought, okay, we need to handle [00:30:00] that like we would if it was a UK secret document that has a whole list of policy. Constraints around that, where it needs to be stored, how it has to be handled.

Mm-hmm. But we went back and spoke to this actual customer and by the word secret, they effectively meant what we would think of was just confidential. Right. Please try not to leave it on a train. Yeah. Best deference, please. Yeah. Yeah. You know, and by this point, you know, our security team, right.Reasonably from their perspective. It's very [00:30:30] expensive. The whole thing about how are we gonna manage this information because of an, you know, thinking that that word would mean the same thing in a different context. So you have to start from there. Those that really quite, in some ways, quite basic understanding, even the things that aren't written down about your assumptions, about how things work, and then build up from there to build that trust and then be able to operate.

That's gotta be awkward at times though, but I suppose it takes a lot of patience and then keep going over it and over it and over it and you'll build that understanding. But if you are, if you are [00:31:00] outside the ecosystem and you have to come in like a new starter and things like that, that's gotta be a very complicated task as well.It's gotta be a, a specialism to work multi-nation state.

It is. And one of the things I find quite interesting, we talked about talent earlier. Where do we find the talent that we need? Well, certainly we need, we need software engineers. We need people with technical skills, with STEM skills, but some of the most effective and capable people.

In our organization and in my team have a humanities background [00:31:30] based on history or international relations. And that experience is bringing an understanding and awareness of some of that wider context that is frankly just as important as the technology in making a transformation program work in that kind of partnership, uh, environment.

So maybe if we just build on that notion of trust a little bit and delve into what that sort of means, maybe. What are the ethics of that? You know, kind of what are the considerations in there [00:32:00] that are perhaps greater than you might see in the, in the more traditional commercial sectors that you have to think about? Sure. So if we think about, for example, law enforcement operator, uh, agencies Mm. Who are trying to understand who is the, the suspect that we may want to go and arrest for, for, for this particular crime. The ability of the state to take away someone's liberty. Yeah. Is, you know, one of the most [00:32:30] sort of sensitive, uh, things that, that, um, you know, government does.o really being able to understand and explain the decisions that are being made and the data that's led into those is, is critical. Right. So, explainability of ai. Is a topic across many domains, many companies and sectors.

Is that the third definition of domain that you just brought into this? No, I think that is possibly, yeah.Third, I [00:33:00] feel you weren't lying. We had more time. I could, I'm sure I get a few more. Um, uh, but that, that concept of explainability. Yeah. I can't think of maybe of many areas. Where it's more important or more critical than in a decision to perhaps arrest or Yeah, to impact it a another human, another human's life.

Yeah. Yeah. So understanding how to achieve that level of trust and assurance of that data and that decision, but without [00:33:30] applying so many constraints to it, that you don't deliver the benefits of, uh, automation and efficiency that these technologies promise. It is central to a lot of our work and tried to apply the expertise that we have from working in these areas for many decades.

And a lot of our people are former operators of, of these sorts of capabilities and really deeply intimately understand what it takes to to [00:34:00] do that job. So we often find ourselves playing a role of working with the technology. A provider to bridge the gap perhaps between the operational environment and needs in areas such as explainability of ai, for instance, and what the technology can actually do, what it's capable of.You know how that can be deployed and use.[00:34:30] So Chris hearing you talk about multi-domain integration data. The amount of data, the quality of the data, are we actually focusing enough on the human capacity to absorb it all? What's your take on that? Are we taking things too fast?

I think the capacity of an operator, or let's say a a, a soldier to take on a new piece of technology or information.

As well as [00:35:00] everything else that they're trying to do in a, in an operational environment is one of the key constraints, certainly. And really thinking about how the technology can be adapted to the ability and capacity of that user in that particular context to take it on is vital to achieve the kind of uptake that, uh, that you would want.

And some element of that will be training and awareness for the user, but from my perspective, a much bigger part of it is. Making sure that [00:35:30] actually the technology is the right fit for that operation and, and not trying to force the users to change. Too much just to make the technology work.

There must be a lot of science that goes into that about you.

You process the data, you work out what the answer is, how you relay that to the human, then could be probably in quite a stressful situation, there might be a lot of other information coming in from all over the place. There's, there must be a huge consideration in these. So we've worked out a thing, but now how do we get the human to understand the thing?

Yes. And [00:36:00] uh. Not within my part of the organization, but my colleagues who work on fast jet aircraft, for example. That's a, an area where there's been decades of research and refinement of the human factors because if you are flying at a couple of hundred feet down a Welsh Valley and with a tiny amount of leeway to make a decision, understanding the best way to get the right information into the pilot's consciousness.[00:36:30]

So that they can make a decision within a, a fraction of a second becomes critical. And if we've got more and more information to present to the pilot, the pilot doesn't have any more capacity to process more than they were already doing. Still human. So. We have to make that better, but still within the, the constraints and limitations that we have as humans.

Yeah. And is it then about understanding what it does, but it's, I think it really also is about trusting what it does. Trusting what the system is providing you in terms of information.

Well, you get that where [00:37:00] a system presents you information and people argue with it. Yeah, classic. My dad used to argue with the SAT nav and say, that's not the best route to that destination type thing.But then you take this context and you go, you've got to really trust what you're being told. 'cause if you're gonna make a decision that's a split second off the back of it, you know, there's a lot of, uh, you can't say you forgot to carry the two in that equation.

Yeah. And I know you've discussed on the podcast previously around.

Things like ag AI and mm-hmm. How that can be embedded and implemented into organizations. And there's, I think, some [00:37:30] interesting analogies about, well, how do we learn to trust other people? Mm-hmm. Yeah. Yeah. And other people telling us information and do we then act on that? And is there something about that interaction, which is quite different from what we've historically done in trusting or not what a, what a computer tells us.

That actually with agent AI wouldn't be somewhere in between. Is there an argument that an agent is more predictable and more trustable in that way and can maybe consume data faster than a person? Yeah, I, I think so. It's somewhere, perhaps yes, [00:38:00] closer to a person, but for all the complexity that we built into some of these agents, probably still less complicated than a than a human. Than a human. Yeah. That's almost certain. True. And, and trust of course, of people and decisions that they make central to operating in the the secure world that we do a lot of our work in. You think about security clearances, we have the idea of can you trust this individual to be able to handle sensitive information based on what you know about them.[00:38:30]

Perhaps there are. Equivalent considerations you could give to an AI agent that helped think about that problem in a different way, right? As a non-deterministic system compared to information assurance as it was before. And, well, how do I know It's a completely predictable, uh, outcome.

There's that whole new thing where they attack the software supply chain.

So before it even gets, you know, the, the, you, you, the. Open source library that's compromised and half a million people download it and then deploy it in their software, and it's all signed, [00:39:00] inserted as it goes out the door. You sort of go, well, how do I trust the supply chain that made the agent that then I'm gonna deploy into us?

That type of context. Well, where did it come from? Who wrote it? What's inside it? And as it been corrupted Yes. What data was it trained on? And we would say the majority of, I think that the, the most sophisticated and damaging cyber attacks we now see are. Supply chain based and if we open up supply chains are complicated enough as it is without [00:39:30] thinking that the supply chain really needs to include all the data sets that that agent was trained on, as well as actually who developed it.

It, it's, oh yeah, sometimes it's easy just to put a human back in the loop and go. They'll check it. Yeah. Yep. I mean, you're talking about trust in these partnerships that you already mentioned, especially across abroad, you know, different cultures, but also, uh, between, uh, civil military, uh, infrastructure.

What mindset shifts do you think are still missing to get those partnerships up to [00:40:00] the level that is needed?

Looking at government and companies working together in the interests of, say, national resilience. Making sure that there's an understanding across that divide. It's sometimes there, but it's often missing.

So an understanding perhaps from the government side that these are still commercial entities that still have to turn a profit in order to survive. And an understanding on the commercial side [00:40:30] of, uh, that mission and purpose that perhaps. Goes beyond just the, the, the day-to-day operations of the, of the business and, and recognizing the, perhaps the importance of their organization within the critical national infrastructure and what, what an adversary or, or a threat actor might see as a vulnerability.

It was a COVID learning, wasn't it? A globalization that we suddenly discovered that lots of little things that can be denied can kill massive systems. Supply chain just for the basics like [00:41:00] food and textiles and whatever else. So you go, you, you apply to this incredibly complicated domain. Hey, toilet rolls Toilet rolls. Who would've thought it? What I still don't get is why people started hoarding them. Somebody somewhere still got a garage full of toilet rolls from 2021. Haven't they bad? They've, they've turned into that. You know that company online where you can buy a box of like 400 toilet rolls? Yeah.It's like COVID. They've, they've monetized that over over purchasing. They'd be like, I know we should just sell 'em in 500 pa 500 roll batches. I mean, let's be [00:41:30] honest. Who buys 500 toilet rolls? Where'd you put 'em? Garage. Yeah. Yeah. They go. But there was that, it's the behavior as well. When things change, people, you've, you've, you can witness quite odd behavior depending on what impacts arrive. Certainly behavior that becomes unpredictable. It becomes unpredictable quickly.

Yeah. So you said people becomes become influenced. Easily and become unpredictable as a result of that past. I mean, if you said before COVID there's a global pandemic, what's gonna be the [00:42:00] biggest issue? Not being able to buy toilet paper would not be the top of my list. No. Would be. Well would it be now though? It would be. You know, people have learned, but no, you still know we're gonna go back anyway. That's on a massive aside. I, I think on that note, well, I think we brought that to a hell of a conclusion. Chris, what do you think? Absolutely. I didn't necessarily expect this to end with toilet roll, but, um, but you know, well, on that note, thank you so much for spending, uh, your valuable time with us today and, uh, giving us some insights into, uh, [00:42:30] a highly complicated world. It was a pleasure talking to you. Great. Thank you very much. Pleasure to be here. Now we end every episode of this podcast by asking our guests what they're excited about doing next.

And that could be something in your personal life, like, got a great restaurant booked to the weekend, or it could be something in your professional life, or a bit of both. So Chris, what are you excited about doing next?

Well, uh, I'm very excited that I've got tickets for the Women's Rugby World Cup semi-final.

Oh, very cool. Very cool. Still very nice. So I, I'm based in Gloucester in the west of [00:43:00] England. Rugby country. And so having the, the World Cup, uh, in the uk, uh, or in England's been um, uh, fantastic. Uh, hopefully we will be England in that semi-final. Apologies. Apologies to Scottish, Scottish listeners. What are their form, what's their form Been fantastic through the tournament so far, I think including the, possibly the record, record points scored in a, in a World Cup match, right.

Um, so yeah, really looking forward to taking my. Uh, my dad and my two [00:43:30] children to uh oh. Wonderful. I'll be a great day out. Amazing.

If you would like to discuss any of the issues on this week's show and how they might impact you and your business, please get in touch with us at Cloudrealities@capgemini.com.

We're all on LinkedIn and Substack. We'd love to hear from you, so feel free to connect on DM if you have any questions for the show to tackle. And of course, please read and subscribe to our podcast. It really helps us improve the show. A huge thanks to Chris, our

sound editing wizard. Ben and Louis, our producer, Marcel, and of [00:44:00] course to all our listeners, see you in another reality next [00:44:30] week.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Make it real.
www.capgemini.com

Capgemini