|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| **Accident vs Intentional** |  | | | | | |
|
|  |  | P10 |  | I think we might be, you know, in that zone already, but just think about news reports. You know, the first, you know, it's not believed to be a terrorist attack. You know, just because you know, if that's how we want to model it, I think it's already already an issue. I think that's a very nice call. Yeah. | | |
|  |  | P10 |  | OK, I I I have a slightly different. So I mean I think working with colleagues at NCSC, they they are very you know, while I work with the sociotechnical and risk team predominantly, they're very good at. So you don't. So the, the, the, the sort of the very the Uber techies which to just assign unfairly different tribes, it's fairly to these tribes. But for them, you know, the humans, the kind of the wet wear, we are the humans are the weakest link and then the sociotechnical risk group. Of course humans are also the strongest league.  I don't have the data to back this up, so I hate throwing this into the mix, but I think I still want to.  More sort of breaches are, you know, are caught by human spotting reporting, you know, than any sort of automated system. And there's really good, you know, a good story there that people are very good at stopping and spotting things. You hear stories that people realising, yes. Yes. They've clicked on the malicious link, but they're also the one who, you know, who it's a it's a it's a it's it's not like you know, they'll just rip the you know they'll rip it out of the system.  And they'll lose. You know, various proprietary stuff. But so it's like people are doing very clever good things in in lots of places. But I think we, we we are a bit more a bit more up to the idea that you know just clicking on those links is is clearly you know that sort of social engineering attacks are are really critical. And I think we've seen the rise in the number of you know is it something that was on the radio yesterday about the number the rise in fraud in fraud.  You know, so basically online fraud as is now the most sort of common motive you know of of sort of criminal.  Injury that that your average citizen encounters, which is clearly digitally enabled. And so I think the seeing that over into crossover into cybersecurity where where people are vulnerable if not that we think certainly vulnerable, yeah. | | |
|  |  |
|  |  |
|  |  |
|  |  | P11 |  | I would go further and say it shouldn't matter whether it's malicious action or failure.  In your first response and if you go to a computer security.  Manual and it tells you that there's a computer security incident response procedure and the first node says determine you have an computer security incident.  I will immediately reject it because in many, many cases where you have a complex only partially observable environment, particularly an industrial one.  The first thing you observe is that it isn't working the way it did earlier, and it's probably what that maintenance tech did, or some idiot on the control panel or something's broken.  And it's about 48 hours later when you've exhausted every other possibility that you might say oh. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 1 of 316 |  |
|  | | | | | | |
|  |  | P12 |  | Oh, that's a good one. Yeah, totally. Yeah. I actually, this is I. I've never framed it so crisply before, but I have wondered this sometimes with like CDN outages where it was this image or you know dot dot dot dot dot 'cause, you know how much like think about this. OK. And again, this isn't like a war thing, but say you're like an Indonesian short sell.  And you have an idea that you know you're not going to get caught on, all you need to do.  Is like get into Cloudflare or pay a cloud flare turn and say hey, can you change this BGP route for like 30 minutes and you you know do something where a big Indonesian financial firm is inaccessible for 30 minutes, make a lot of money on your short position exit your short position and then the issues are stored Potter says oh we're investigating but it just seemed to be a misconfiguration and you've made millions of dollars potentially.  Would you actually get caught? Like I really don't think so.  So yeah, I I do think that that I think that that's actually very possible. And I also think that the more this is going back to AIA little bit and the more kind of way that I think about AI, when I look at AII really see this is almost like the way I would look at like a compiler where like we had assembly, right. And then there's this compiler that's interposed between you and the actual assembly code.  And as you work your way up that stock, you know with Python I don't even know what's happening at the C++ binary layer, let alone what's happening assembly. And now I think like AI and generative AI in particular has really interposed at a level above where, you know, I know people who are using, you know, llms to generate Python. And that's just another layer of interposition. And I think that as AI interposes more and more in that stack, the more it becomes difficult to discern what's actually happening. And I think to this question, yeah, that does potentially make it harder to discern whether something was.  Misconfiguration or yeah, an an attack. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  | P13 |  | No, I don't know about that one, I mean.  Can you distinguish between an accidents and malicious activity?  Probably not. If you. I mean, if you have, that's true of anything. If you can't see what's fundamentally caused it.  Now all you see is the end result.  Then it's impossible to tell whether someone has made a mistake or someone has deliberately done that. It's it, I suppose. It all comes down to.  Knowing where something has come from and being able to trust that ultimate source of the thing that generated that, and if you can't trace something back.  Then you probably shouldn't believe that, and I suppose looking at the medical domain.  This is where we kind of have hierarchies of evidence as well, so. | | |
|  |  |
|  |  | P14 |  | Exactly. Yeah. And so there are areas there CBRNE and the like, which is really tricky. Yeah. Yeah, so.  I can imagine that AI and ML and.  CMI glitches could be being caused by all sorts of things and trying to attribute that is quite important. | | |
|  |  | P14 |  | So one of one of the I started that process by talking to stakeholders, asking them what their concerns were.  I won't say who it was, but I had, you know, key influences and people who really should know the answer.  We really it's difficult to tell.  The attribution if something's space weather.  Some a malicious attack.  Or an accident.  Or just something going wrong with the kit. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 2 of 316 |  |
|  | | | | | | |
|  |  | P14 |  | And developing the capability to attribute at speed is really important and it's difficult to do.  I did something and there's another thing I did something on bioterrorism where again. And you think about that poor chap, Skripal.  A policeman's called to an accident somewhere. Someone's fallen ill in a park, or several people have fallen ills in a park, and how quickly can you tell if it's just food poisoning or a major chemical or biological attack?  And the ability to attribute at speed would be really helpful for the poor sod who has to go and rush in to help. | | |
|  |  |
|  |  | P14 |  | So can you get the audit trail and establish what the Hell's going on? And do you have the sensors and and and what's needed will vary depending on what the challenge is. But part of it is about sensing. Part of it is about years and years ago, I was.  Literary not just a different century, but practically a different Stone Age I was. I was.  Posted into BT as security adviser to the head of Director of Security and BT had them. This is in the 1990s. It still exists. The most amazing place at Oswestry where it was always being used in James Bond films because it had huge Bank of TV cameras as as as screens that could then be so the bad guy would always be pacing up the inside his volcano or whatever. Plotting the end of the world and they'd had stuff shown on that. But what they're using it for, for real.  Is they have sensors now then this is in the 1990s, it was. I was really amazed. Great knowledge management. | | |
|  |  |
|  |  | P14 |  | In every one of their exchanges and on their whole network. And these sensors were monitoring second by second volumes on those on the network and they would flag up go red, orange or whatever if a particular network node was becoming under pressure.  So these people were working to then divert bypass. | | |
|  |  | P14 |  | And the way and one of the more amusing things they had was in addition to the screen sharing all of that.  They and international as well, by the way, they had every TV channel playing because what they were looking out for was something that had crashed the network.  A few years before.  Suddenly, everybody is phoning that number.  And if they didn't get that intelligence back to the attribution thing, they think it was a major crisis on the network because suddenly a particular area is flooded. | | |
|  |  |
|  |  | P14 |  | And and so they were having to. Ideally BA should be warning them that this was going to happen. Of course, they didn't always do that. So they were keeping a weather eye on an advertisement that suddenly included a number so that they could try to be responsive to it. | | |
|  |  | P16 |  | I think people, maybe people from the outside, they would be very suspicious. So when there is a an outage of cell coverage for example or electricity, people tend to see cyber attacks everywhere. When sometimes things are more responsible for.  Services and cyber attackers. I think that people, you know, people within the critical infrastructure like think mostly.  They still remain able to differentiate between.  A hostile cyber attack and an accident. I think we still have.  Pretty good visibility of their systems and they've got some good experience and I think I don't think we're at a stage where when it's hard to to distinguish, maybe with AI it's gonna change that.  Attackers are gonna be able to use AI tools to make something look like an accident. When it was in fact, but I think for now I I don't think it's an issue for the operators themselves of critical infrastructures. It's I think it's more an issue for public opinion and and people becoming very suspicious and you know, I kind of.  Conspiracy theories all around the world, seeing all kinds of.  Nasty things happening when it's it's just like. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 3 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | Excuse the the wording, but \*\*\*\* \*\*\* from inside and so yeah, so I don't think it that, that's. Yeah, we're there yet. | | |
|  |  | P20 |  | I think it's becoming ever more complicated. I mean, that's compounded I think by our collective changing media environment as well where you don't you well, we don't in, in my view we've moved away from relying on a few trusted news sources to people relying on all sorts of information channels.  The the non mainstream media as as as they're referring to themselves, Internet platforms which are disseminating news, putting out strategic narratives, putting out political narratives which support particular country or leader or point of view. So when you when you, you know, come to responding to a bad incident, you don't just have you just not just looking at the New York Times or the BBC or whatever.  Which in my view are more traditional, historically trusted media outlets. You're searching from information on the blogosphere and the Twittersphere and all the crazies come out of the woodwork and they muddy the water and they create confusion around it, which again AIDS plausible deniability and respond actors having to take responsibility for stuff. I mean, look at all the misinformation, disinformation about the sabotage involving.  Gas pipeline.  Just to Rush and Nord Stream and things like that. You know the amount of different narratives arts the US, it was the Russians, it was the Ukrainians, right? Who do you believe?  So my point, I guess is that the the general diversification of the media environment is, I think one of the prime forms of complication around that. And then of course, if you want to include cyber and AI, those are all multiple players and amplifiers for that stuff.  And I think you know the the other concern is.  And I had this conversation conversation at a workshop. | | |
|  |  |
|  |  |
|  |  |
|  |  | P20 |  | it's the debate about who do you hold hold to account for? Accidents involving AI? Is it the user? Is it the developer? Where, who? Who ultimately holds the risk the responsibility for when things goes go wrong? And I don't think there are clear answers to that.  Internationally.  In terms of our domestic regulatory environments, I think that that's a very muddy field again.  And I think that worries government. So I would agree, yes, that that is a a trend and and I think it's again that combination of changes in the media environment with changes in the technological environment. | | |
|  |  |
|  |  | P20 |  | Yeah, that's an interesting one.  I think one of the things that disinformation and AI and Cyber does is create plausible deniability.  So if there are, if there are accidents or incidents, then it's easier if they're happening as a result of activity on very opaque Internet networks, it's quite easily easily explained away by national governments, as you know, not our fault. It was a malfunction, blah blah blah.  So I think liability, negligence, corporate responsibility, governmental responsibility.  For incidents and what causes them. | | |
|  |  |
|  |  | P21 |  | But if you're a reader of fake news and you've been influenced by this information, I think then it's harder.  Yeah, I I partially agree with that statement. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 4 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | But I see that as a as a trend.  I actually think in sort of an an offensive side of the term. So we've become relatively.  We've become better at doing technical attribution on identifying who's behind things, and we've also seen more public attribution of cyber operations. And then sometimes you have in case of a ransomware, the attacker more or less makes known who they are, at least in terms of an affiliation of an anonymous group. So in these instances I would say you can distinguish between accident and malicious.  Actor, that sort of more on the cybersecurity front, I'd be. I think it's harder on the disinformation front to distinguish between that. | | |
|  |  |
|  |  | P21 |  | Yeah. Yes. And also because you as the recipient have very little if you're a victim of a ransomware incident, you know that you've been a victim of ransomware incident most of the time, at least if you're a direct victim, perhaps less so. If you're waiting for your surgery in hospital, you might do that because it's the NHS or because that's been offensive where attack. | | |
|  |  | P22 |  | Well, you know, they're both of either a, you know, an operator who wasn't trained properly or some little boy in Bulgaria having fun. But it doesn't matter. The end result is user hours lost. Go track it down.  Measure it, measure it, measure it, measure it. | | |
|  |  | P22 |  | So you have to deal with both. | | |
|  |  | P23 |  | Yeah, the the systems approach, I mean, I think it's, I think there's a clear in the literature there's a clear understanding that we need to do systems approaches.  But the law doesn't always require a systems approach.  Evaluation of human in the loop machine interaction.  So yeah, so there's a lot of you, I think you wanted to talk about technology, but I've mostly talked about kind of problems in law. | | |
|  |  | P23 |  | And about and this is something about the human computer interface, isn't it as well that that, you know, the Tesla one?  It is is somehow you're not.  You're not looking at the the combination as a system, but you're saying so long as you know the car was in control, now you're in control and they're two different situations.  Instead of that handover is itself a disaster.  He he is a is a thing that no, no system should do and yes. | | |
|  |  |
|  |  | P23 |  | And then when you figure out what happened, you see they're kind of both at fault and you have to make normative decisions about who should be responsible for what.  And and the these are these aren't easy to solve it.  I mean, the interesting thing about Tesla, right?  It Tesla says we don't have accidents and one of the reasons why is because they they turn off autopilot right before an accident is about to occur.  So you can be like blah.  Gonna drive it along and then literally with one second notice it bings you have to take over and avoid an accident.  So Tesla has a very kind of, but it I mean it's it's basically, you know, it's disingenuous. | | |
|  |  |
|  |  | P23 |  | You're there's so not in practice, but there's a very interesting literature on the problems and testing and evaluation.  Umm that, yeah.  In a machine learning systems, you know there's a there's.  If you read the studies of the 737 Max.  Yeah, I think about other software accidents.  All the Tesla accidents too.  I'm the there is a kind of thing that happens where the system designer blames the operator.  The operator blames the system designer and it's very expensive to figure out what happened. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 5 of 316 |  |
|  | | | | | | |
|  |  | P8 |  | If my people, if I measure something like this around this, isn't it? So it's more like it's very difficult to distinguish between a fault in the system and a malicious like an attack. So a lot of people, I don't think we are really trained, we can really distinguish the difference between what went wrong and why it went. So we may understand what happened. Like 2 cars are crashed in terms of why that happened. I personally believe.  We will not be able to be able to say that unless we really trained and we actually know what to look for.  Some people we know it very well because they know what to look for, like some of them are like an experts here. We are trained partially for that but is much like in every job. No, no. It's really very hard to know. Yeah. And this might be, yeah. | | |
|  |  |
|  | | | | | | |
| **Accidents** |  | | | | | |
|
|  |  | P11 |  | What we're actually talking about is how do we make?  The critical infrastructure of the future, resilient not only, I think against.  Adversarial action.  But against failures. | | |
|  |  | P6 |  | Whatever crisis disasters in natural disasters.  It was out there a little bit, but it was never priority in no state we didn't spend.  Enough attention to it priority as societies all over Europe, I would call it. It was out there. Researchers were there, Ng OS were working there, but we didn't make it serious enough. And and the private market.  Did not invest in this kind of resilience because it was not necessary | | |
|  | | | | | | |
| **AI and Cloud** |  | | | | | |
|
|  |  | P11 |  | and the final thing is the use of cloud cloud based services, particularly for sort of diagnostics for what's that expression. One of my colleagues uses.  It it's sort of, it's looking backwards and looking forwards. I can I wish I could remember how he puts it so elegantly, but it's like it's like predictive maintenance and diagnostics. It's looking in both directions based on.  The sort of things that cloud based systems and machine learning do so well. | | |
|  |  | P14 |  | So all I can do in a sense is just report back the insights that I get from.  My community that I speak to, and I suppose it's going to be very obvious answers AI, machine learning quantum.  Probably I'd try up at that point, even though the people I spoke to might have huge months more to say on that, you know, they might come up with others, but you know those AI machine learning quantum are the big issues. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 6 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **AI and Technology for Incident Management** |  | | | | | |
|
|  |  | P15 |  | And therefore I think anything around making, I think there's a potential for.  Comms and information sharing and technical information sharing.  For situational awareness and response and decision and making good quality decisions based on as much information as well, not as much information as possible, can source it possible to get overwhelmed by information, but normally you end up not having enough and then you have too much of it.  And therefore, like there's a, there are opportunities I think for technology and technological advances to.  To aid those processes, | | |
|  |  |
|  |  | P15 |  | emergency alert thing that went on.  And there have been various sort of activities to look about how how you can push out information to people particularly I think it's probably less relevant for CNI because you're not going, there's not a large event, but for like large public events where there are huge numbers of people in the centre of big cities and things like that, it can be a useful way of pushing out information and instructing people on where to go and where is not safe. | | |
|  |  |
|  |  | P15 |  | Except for, except for things around I don't know, like drone technology and having better situational awareness from like aerial scene understandings and and also things around pushing out messages.  To to people. | | |
|  |  | P16 |  | Probably try to design new systems that are not fully automated but work hand in hand with humans to kind of monitor and respond to cyber attacks in a way that's really effective for organisations. | | |
|  | | | | | | |
| **AI Arms Race** |  | | | | | |
|
|  |  | P16 |  | the AI will also be able to test.  Systematically, all the vulnerabilities of all the systems that we deploy. So, so you have AIS being used to craft malicious software to attack malware and of course we'll have AIA is to defend us, but then there will also be exploratory Ai's that will scan systems all the time and try to identify the thousands of vulnerabilities that are.  Introduced by coders because you know no human is perfect and everyone makes mistakes. And when you you write a piece of code that has like 5,000,000 lines of code, then every thousand line you're gonna introduce.  A mistake, an error, and then those Ai's are gonna be able to document systematically all the all the points of entry. So. So we're gonna have like also a new level of.  Vulnerability. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 7 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | The kind of identified by A is because they're going to be able to systematically map and document and exploit probably those vulnerabilities. And of course, hopefully we'll have empty vulnerability. AIS are going to be able to also help us fix and identify those vulnerabilities vulnerabilities. So again, it's going to be another arms race, but I think that in terms of the.  The gaps that we have in our existing digital infrastructure and then the the attack cycles on the other hand. | | |
|  |  |
|  |  | P16 |  | But you can imagine that they've refined.  A lot of that perfected their systems and that's happening and that this kind of.  Malicious software against defending software arms race is underway and.  Where it will take us and how far it will kind of go, no one knows | | |
|  |  | P16 |  | So for AII think it's gonna be, you know, massive probably.  Communities for cybersecurity companies trying to offer products and services to the critical infrastructure to adopt those new technologies | | |
|  |  | P23 |  | there's there's all these reasons to think that cyber could be defense dominant, but on the other hand, I think the, the, the kind of technical thing, the technical challenge we're facing now is that it's becoming easier and easier to become an attacker. | | |
|  |  | P3 |  | the applications are things like machine learning.  To I don't know for optimization predictive maintenance, you know, those kinds of technologies.  And of course uses of machine learning for cybersecurity, right? | | |
|  | | | | | | |
| **AI cyber attack** |  | | | | | |
|
|  |  | P12 |  | Yeah, definitely. Yeah, for sure. Yeah. Well, the only thing we could help is that the only thing we can hope is that those same tools will be available to the Blue team so that they will be able to, you know, yeah, foresee that kind of stuff better. But yeah, for sure. And, you know, this goes back again, so many of these things are social issues. But, you know, just like responsible disclosure stuff is really hard and, you know.  Yeah. Like, I think identifying vulnerabilities isn't assigning them acvs score like that loop should be improved tremendously by AI. So I'm actually that's one thing where I'm optimistic in aggregate that it will actually help people. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 8 of 316 |  |
|  | | | | | | |
|  |  | P12 |  | When it comes to the because you mentioned malware, I will say on the malware front alone I am optimistic because I think that those AI tools that help generate malware will also help identify really bad vulnerabilities and especially vulnerability chains.  'Cause that's also. I'm sorry, I I've really got me talking and I understand also it's late for you and early for me. So I'm like drinking my caffeine. You got me as motivated but but you know, I think like the vulnerability chains are always really hard I think because you get often when I what I observe is that you get either these really, really great research hackers who know everything about like ARM architecture, right or you get these really good operational hackers who can really like chain existing vulnerabilities together. But what happens is that OK you get this researcher who can come up with this vulnerability.  And then they themselves will not be able to put together. Oh, and the reason why this is really bad is that I can do this chain where you know this exploit chain that gets me somewhere else. So what? This ends up happening, you know, in, in, in state. You know apt is where they are the ones who are able to do this. But us we are mortals are not able to piece together the real consequence of any vulnerability that comes our way. So it looks like a low C VSS may in fact be really really big deal. So what I'm hopeful for is that with these AI tools we'll be able to do more.  Automated exploit chaining.  In a way that makes it more obvious which vulnerabilities really matter and which ones are just kind of like you can't actually get that like log 4 J seemed really bad, didn't actually turn out to be a big deal.  So yeah, that's what I'm hopeful for. I'm an optimist on this. | | |
|  |  |
|  |  |
|  |  |
|  |  | P13 |  | Maybe I think, yeah, it's, I mean, obviously healthcare depends on these kind of systems and if that's happening on these systems, then it's a problem, but I wouldn't consider it a problem specifically with healthcare domain.  No, it's not. | | |
|  |  | P13 |  | Yeah, you kind of need Amazon to be defended against this, but you'd not. It's not a it's not a local problem to healthcare, it's it's the same for everyone. Yes. Yeah. OK. | | |
|  |  | P16 |  | They they've only refined and that's, you know, the stuff we don't know, of course, because it's all classified. But you can imagine that they've refined.  A lot of that perfected their systems and that's happening and that this kind of.  Malicious software against defending software arms race is underway and.  Where it will take us and how far it will kind of go, no one knows. But there is all. There is the arms race and there is also the fact something also connected but slightly different is that the AI will also be able to test.  Systematically, all the vulnerabilities of all the systems that we deploy. So, so you have AIS being used to craft malicious software to attack malware and of course we'll have AIA is to defend us, but then there will also be exploratory Ai's that will scan systems all the time and try to identify the thousands of vulnerabilities that are.  Introduced by coders because you know no human is perfect and everyone makes mistakes. And when you you write a piece of code that has like 5,000,000 lines of code, then every thousand line you're gonna introduce.  A mistake, an error, and then those Ai's are gonna be able to document systematically all the all the points of entry. So. So we're gonna have like also a new level of.  Vulnerability. | | |
|  |  |
|  |  |
|  |  | P16 |  | Yeah. I mean, for me, that's a given. So no. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 9 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | The kind of identified by A is because they're going to be able to systematically map and document and exploit probably those vulnerabilities. And of course, hopefully we'll have empty vulnerability. AIS are going to be able to also help us fix and identify those vulnerabilities vulnerabilities. So again, it's going to be another arms race, but I think that in terms of the.  The gaps that we have in our existing digital infrastructure and then the the attack cycles on the other hand. | | |
|  |  |
|  |  | P16 |  | I think that's something that I mean, I remember the DARPA, the American.  Research Advanced Research Programme Agency organised five years. Was it five years ago in Las Vegas, a competition of.  Autonomous systems attacking each other and defending each other, and and they weren't as far to create a new computer language to make sure that those systems didn't leak into.  You know real.  Out the real Internet or real tech system so that it couldn't be weaponized, but.  The organisation organised that kind of competition. It's not out of sheer curiosity. You can imagine that they are planning to to use that and and I attended a presentation. I think it was six or seven years ago, maybe more of a big tech company explaining to us that they were using those systems already to Red Team to attack their own systems.  As Red Team, so instead of hiring you know humans only, they also programme their own attack machines to attack themselves constantly.  To to test the the you know the boundaries of their protection and their the reliability. So if so, if if that was possible 10 years ago, you can imagine that now. | | |
|  |  |
|  |  |
|  |  | P8 |  | Might might be I am not dead. How shall I say of like knowledgeable in terms of specific or mother and so on. However, any sort of malicious kind of like attack and pet, much like an art comes of it. If Marvel whatever done I will say like an AI will make things a bit more tricky. So that's what I can say only yeah. | | |
|  | | | | | | |
| **AI Enhanced Attacks** |  | | | | | |
|
|  |  | P10 |  | I think that is it's it's the way that llms I'm going to not say AILM sort of sort of.  Put the standard threat models sort of on steroids, you know, so just in terms of kind of pace and speed and and range and and sophistication.  And I think that's actually the the area that I think is a significant risk. | | |
|  |  | P16 |  | Because the tool they have at their disposal has some level of, I wouldn't say consciousness, but has some level of autonomy and automation that will actually that makes it.  Do things at a scale that.  An untrained or unskilled mind cannot comprehend.  So they just see, you know, a machine able to.  Achieve certain things, but without fully comprehending that how it it it's doing that and then they're not understanding the all the all the implications of their request in terms of.  Neutralising or harming the whole you know the the the targets systems. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 10 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | Malicious activities against critical infrastructures.  We've heard about it for 10 or 15 years. As you've read in the report, and some use cases and people used to make predictions, but I think now we are starting to see the adoption of AI technology by attackers to.  Identify vulnerabilities of critical infrastructures, craft pack tools or design some.  Customised messages for victims of spearfishing or fishing attacks. | | |
|  |  | P16 |  | we are starting to see some.  Live examples of AI being used to.  Support some. | | |
|  |  | P17 |  | And then likewise you've got the you know you've got the deep fake voice and or even the physical, you know virtual online calls basically. So you know if you've if you've got someone your line manager tells you know Bob who works on the workstation and connected to the PLC that looks after the nuclear fuel rod and said look we've just had confirmation we need to adjust it by .1% and Bob thinks OK fine that seems like a relatively OK tolerance.  And does it and it causes a hazard, then obviously you know that could be something that we're we're going to see soon, I think | | |
|  |  |
|  |  | P17 |  | so phishing attacks quite straightforward. You know it's it's, it's kind of penetrating the human factor aspects, you know, using sort of crafted.  Crafted emails that look and feel like they're sort of genuine.  Can or cannot contain certain items within the the the the metal kind of protocol that that could potentially infiltrate and and cause.  Big impact into your network. So we are seeing as a couple of cases now where sort of the use of AI is actually permitting aspects about the e-mail protocol. So that a can slightly avoid some of those defences. So things like where we have not just spam filtering but.  Certain male rules that we have in like exchange. For example, there's there's things about that that's starting to kind of change a little bit and then obviously the the way and look and feel of the, what's it called, the actual emails themselves, it's not just, oh, let's do a copy of O365 login sort of thing and make that quite, quite rendered sort of thing there. There's there's lots of tooling out there that can sort of detect whether that's, you know, looking even if it's come from like what looks like a valid source, they can sort of look at the e-mail content and say, yeah, this is crafted a sort of.  Remarkably look alike. | | |
|  |  |
|  |  |
|  |  | P17 |  | These guardrails are off, so it's pretty much, you know, what can you do sort of thing? And I think that will drive a a a bigger incentive to to make attacks a bit more successful from that perspective. So that's my concern is that actually you've you've always got the seesaw effect and we're always sort of slightly up in the air because the weights tends to be on the opposition side, if that makes sense. So I feel like this potentially probably adds a little bit more to it. And yeah, as much as we want to sort of regulate AI and and other sort of kind of mechanisms.  To some extent, that might even regulate the tooling that will protect us as well. Whereas the tooling used by adversaries might be off bounds completely, so, you know, doesn't matter if you've got regulation, it might even hinder it. So yeah, so that's some of the concerns I think. I think that that's definitely an area of concern from my perspective. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 11 of 316 |  |
|  | | | | | | |
|  |  | P17 |  | One of the benefits of AI or Gen AI should I call it is you can you can upskill people who don't have skills if that makes sense. So you know, I mean I can write, I can write software code that's not a problem, But I'm I'm not the best coder in the world, but I can. I can write quite a few languages.  Some better than others, but if you don't know how to write code, you can generate code quite happily. You could probably build a fully functioning application that otherwise without Jena and AI you wouldn't be able to do at all. So when you then throw that on the opposite side of the fence and we're already starting to see this and it's it's all been predicted as well, a lot of things like, you know, the sort of attack vectors that we're starting to see are starting to use more clever, sophisticated ways and use an AI to sort of help generate.  More sophisticated code sets.  Obfuscation and so forth. So I think that's only going to increase when you look at the attack vectors that are there today and how AI can influence that. I think that will obviously add a massive technical advancement in that area, which will mean that making attacks will be a lot easier from from that side of the fence. | | |
|  |  |
|  |  |
|  |  | P17 |  | if you've used generative AI tools online and so forth or offline, just like I have you know, there are restrictions in place to stop you from getting it to do. There are ways to get around that and there are ways to sort of bypass it in some instances, but generally speaking the restrictions in place because there's a sort of not a regulation but a set of guard rails to make sure that we don't abuse it basically. But in sort of the opposition side of it where you've got attackers that want to use it. | | |
|  |  | P17 |  | But yeah, in terms of concrete examples, I mean we're we're certainly see it on, I mean it's not necessary to do a voting although OT does suffer from you know the the kind of as a Lockheed Martin did you know this kind of two step prong attack which is infiltrate through the IT system.  Infiltrate the OT systems, which tend to be air gapped, or or somehow disinciled from enterprise it. | | |
|  |  | P17 |  | But AIS have been used, and we've seen a couple of cases where that's trying to actually modify it. So that actually it still comes through and to the end user, it looks quite genuine. So there's that example. I guess the second example, which we all know of now, which is you know, you only need to sort of record a 15 second clip of your voice and a picture of yourself and then you've got deep fake.  Defects which which was used against a Japanese bank official, which which obviously lost him a lot of money. So we we called out.  I mean you have BC which is business e-mail compromise, which is where you you you click on a link some individual in a in a business and then it leads to.  You know, either an account takeover, a foothold for the attacker and then they do a lot more and that leads to business to count takeover basically. So they they pretty much take over your business.  So I mean with deep fakes, I think that's going to definitely enhance itself because it's quite easy like anyone can do it realistically. I mean if you've got a few minutes you could you could do that. I think that's something that's a bit of a concern. | | |
|  |  |
|  |  |
|  |  | P20 |  | I think the other obviously major challenge, which probably most people talk about now is AI, both in terms of how we use automated processes and systems for critical national infrastructure protection, but also, you know, I'm particularly interested in. And as I mentioned, I'm doing research on the security of AI itself and how AAI might be weaponized to harm critical national infrastructure either through.  You know automated self learning, self replicating.  Facts the the engineering of malware, which might be particular that particularly damaging to industrial control systems. | | |
|  |  |
|  |  | P21 |  | In our research, there hasn't been evidence for any systematic exploitation of that data, primarily because cyber criminals don't have to, because they're money driven, they have easier ways to make money. It doesn't have to be that complicated.  And there's that amount of data that they harvest is also it will change. I think with AI and better and more computing and passive.  Do you? But it's quite an effort to sort that data to analyse that data to then turn it into something that you can use for further crime, right? So that amount of effort and storing that data in the 1st place and you have to pay for that and so on and so forth. Yeah, that is currently not being exploited to the extent that one might fear. But I think that is something that could very much change if there's different data analysis capabilities. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 12 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | AI certainly perceived as a tool for cyber criminals to launch more targeted.  And highly individualised fishing attempts, for example, in a in a faster way. Also that it expands their ability to target areas that were previously perhaps unlikely to be targeted, for example.  ChatGPT as a large language models being perceived as an opportunity for cyber criminals to expand in areas where they've previously not been able to speak the language. Japan being a prime example.  And we were very culturally sensitive and complex language.  And previously Google Translate for example just wouldn't wouldn't translate to an extent that that would make for a believable phishing e-mail. Whereas with increasing ability of large language models to.  Mirror that language, including cultural references and cultural context. That sort of the fear that that would have mean open up new.  Pockets effectively for sagaminals, | | |
|  |  |
|  |  |
|  |  | P23 |  | There's essentially automated and near automated packages that very unsophisticated people can download and use, and then the question is, could we imagine a future where there's automated packages are trained with machine learning umm to find unknown?  Unknown ways, then.  So these are the this kind of we so like the trends I see is we could have more attackers because it's getting easier.  We could have attackers that are using automated attacks, which stinks.  And then could we imagine a future where critical infrastructure is experiencing completely novel attacks that are intuited by an autonomous system?  These are the kind of work very worrisome trends that are near term, that like next five years. | | |
|  |  |
|  |  | P3 |  | You know, there's a lot of talk about using sort of generative AI mean it's not necessarily images to improve things like social engineering.  And in in this sort of space, then sort of maybe more on a kind of technical level, there's a whole class of attacks to control systems around manipulating input to them. | | |
|  |  | P3 |  | You know, one of the kind of attacks that you know, like the Mission Impossible thing where you replay a video, you know, while somebody's doing something, you know that that kind of thing.  But using AI and generative AI to sort of generate images of something normal behavior or whatever, that's the kind of an idea that's sort of been floated.  Umm, which is sort of very kind of and Terry, practical or perhaps not very exciting. | | |
|  |  | P5 |  | It's gonna absolutely become a much bigger problem, I think so, yes, I would absolutely be focused on one of those, that technology.  With the trust issue in the Truth ground truth. | | |
|  |  | P5 |  | we talk a lot in the past about an operator sitting at all of his screens or her screens and looking at the data.  And do you trust the data or not?  How would you know if it was right or wrong, you know?  And So what are those other systems that may not be digital that you think you do trust, which are analog, that you can compare at least or something like that and with all the deep fakes with the AI, with all these things that are just coming on the ICT side of things, it's gonna work its way into the operational technology.  It's gonna work its way into the nuclear world. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 13 of 316 |  |
|  | | | | | | |
|  |  | P7 |  | Yes, I think that's potentially a very big area and and a very big problem because now you know if you are on the defensive.  You not only need to have you know AI to, to defence, to defend against.  Things happening, but also to be able to defend against deception, which is, you know, a very yeah.  Yes, a very complicated.  Very complicated thing.  Engineering that is quite quite often involved in cyberattacks.  Again, can be weaponized by by AI.  You know, imagine, imagine how people are being fished, you know, through through, through fishing attacks, without being so intelligent. But still people fall, victims of it. Imagine if it's, if it's even more more weaponized. So, yeah, I think I think that's a big problem. | | |
|  |  |
|  | | | | | | |
| **AI for Incident Detection and Prediction** |  | | | | | |
|
|  |  | P16 |  | We're gonna see a lot of uptake uptake and critical infrastructures and the banks are doing it and they've been doing it for a for a while. So they're not, it's not a surprise to them. It's just like still probably very murky in terms of determining which products or services or use cases actually makes sense for them in from a security delivery perspective. So you know is are the new technologies that are being promised to them to enhance their.  Cybersecurity posture gonna be useful, or they're gonna create more work.  And by generating too many false positives and and so on and so forth. So I think that, man, it's gonna be probably.  Major efforts on the parts of critical infrastructures to.  Embed AI technologies into their cybersecurity solutions and. | | |
|  |  |
|  |  | P16 |  | Probably try to design new systems that are not fully automated but work hand in hand with humans to kind of monitor and respond to cyber attacks in a way that's really effective for organisations. | | |
|  |  | P20 |  | That balanced against how effectively we can harness AI for automated defence of these facilities and installations, which as you know other researchers probably are, are doing research on at at Lancaster again with regard to nuclear security | | |
|  |  | P21 |  | the opportunities for AI in a cybersecurity context are often overlooked in terms of vulnerability detection, patching and so on. AI can also work as an enabler for cybersecurity for the good side, so to speak. | | |
|  |  | P22 |  | Particularly in critical national infrastructure, there might be the interest in developing monitoring of performance of systems to pick up advanced warning. You know all events, events that don't happen, you build up the data and actually using AI to analyse those could be a very important use of AI going forward.  And they suspected that most companies in the critical national infrastructure hadn't yet started to think that way. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 14 of 316 |  |
|  | | | | | | |
|  |  | P22 |  | I mean the nuclear industry learned that it was only by looking at near events that you actually could get a sniff of what might be a catastrophic event.  And when you've got people watching it, it usually doesn't happen. But that's the big opportunity for AI that AI could build up this pattern much better than humans can do because, you know, humans are on shift or off shift and, you know, somebody may not say to the next person I was watching that lightning went a bit flicker. | | |
|  |  | P22 |  | but to me it seems this seems an application with all with very much plus side, whereas things like recruitment using AI seems to me to have very much negative side because it locks in historical patterns and you know, as a scientific woman, you know, I'm not happy with being recruited on, you know, criteria for recruiting scientific women in the 60s, you know, which is where out of data originates whereas, you know, if you're tracking faults, you know, having a historic track is actually what you want.  And so please do AI strengths rather than locking in weaknesses. | | |
|  |  |
|  |  | P23 |  | one topic that frequently comes up is whether machine learning.  So whether AI will pitch cyber to be offense dominant, but actually I think it will be defense dominant and the reason why is that machine learning requires lots and lots of data and in fact we have tons of data about attacks.  We like tons and tons of network data.  We can even detect perturbations to software.  It's all be done in machine learning.  Antivirus, for instance, is a huge machine, learning based success.  Well, relative success, right? | | |
|  |  |
|  |  | P5 |  | But, but what about, you know, zero day malware that's out there that you've never seen before?  That's where the AI is going to come in and look for patterns, right?  Look for those things that that things could be not normal.  So yeah, I think there's a lot of research that needs to still take place on the AIC side, looking for malware that's never been seen before. | | |
|  |  | P7 |  | These are signatures that are nonobvious. You know, it's not like I'm I'm. I'm flooding your link. And you, you see, excessive load and you can you can do something about it. If not too late.  So I think AI has a role to play there to come back to your to your question, I think AI has a role to play there. | | |
|  | | | | | | |
| **AI for Information Sharing about Software Design** |  | | | | | |
|
|  |  | P4 |  | I mean, one of the things that that we are looking at the moment is that given that the knowledge that people need to have is quite special right now is quite specialized because this stuff is not getting delivered in universities.  The expertise is in the heads of a limited number of people and their time is very, very precious.  How can we use automation so that we can make the most the best use of their time?  Uh, because we can't lick as literally if we are going to.  If we change the configuration of a sort of platform and we go through the certification pipeline and it takes weeks. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 15 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **AI for Risk Management!** |  | | | | | |
|
|  |  | P15 |  | having a better understanding of how previous risks have manifested themselves and and learning what other people have already learnt | | |
|  |  | P15 |  | So I think there has to be a way like if there can be a way that technology can.  Enable the limited human resources to be more effective in what they're doing, so they're not spending. They're not all spending a day looking at this risk and doing the same thinking they can get that thinking from because somebody else has done it and they shared it with them or whatever it is.  If technology can enable smaller number of resources because unlikely, we're going to magically just get loads more.  Then that would be useful also better understanding. | | |
|  |  |
|  |  | P6 |  | Where our data so the architecture is understood, the system can help me and say OK can help me by the risk management if you do it that way. At the end security it's all about risk management. I will not answer the tools can help the engineer how to put the system from scratch that we've tried to prevent as much as possible. Vulnerabilities, wrong architectures, wrong system decisions. It will mean a higher cost at the beginning.  But it will decrease the cost at the end for testing and verification and all that we are doing today and we'll also have more resilient systems and this is not yet there in any kind of, I would say public organisation or large critical infrastructure operators and that's the challenge that they have. | | |
|  |  |
|  | | | | | | |
| **AI misinformation through social media** |  | | | | | |
|
|  |  | P11 |  | No client nobody knows what to do about it. Nobody really knows how to put a watermark into something to say this really hasn't been.  Tampered with because?  Ultimately, it's not the technology that you're trusting, it's the person who's operating the machine. | | |
|  |  | P11 |  | So I was asked recently what worried me about AI. And I said I thought that it would.  To greatest schisms in society.  A couple coupled with the way that people get their news because.  You end up losing trust in any source of truth.  And as soon as we get beyond a certain point, it's going to be very difficult to reverse the only basis of trust that I can conceive of is trust me, because I'm trustworthy. Because you know me.  And I think that this kind of fabrication of very plausible mistruths will lead to a world of each of us living in our own little echo Chamber of our own prejudices.  I think people are recognising that. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 16 of 316 |  |
|  | | | | | | |
|  |  | P4 |  | I've got a colleague of mine xxx who's there, who's literally all about disinformation and the impact that it can have on a on on autonomous decision making and how bad, how bad people could cause, sort of, how that could lead to bad people causing things causing harm effectively. | | |
|  | | | | | | |
| **AI to Analyse Software Vulnerabilities** |  | | | | | |
|
|  |  | P12 |  | I will say on the malware front alone I am optimistic because I think that those AI tools that help generate malware will also help identify really bad vulnerabilities and especially vulnerability chains.  'Cause that's also. I'm sorry, I I've really got me talking and I understand also it's late for you and early for me. So I'm like drinking my caffeine. You got me as motivated but but you know, I think like the vulnerability chains are always really hard I think because you get often when I what I observe is that you get either these really, really great research hackers who know everything about like ARM architecture, right or you get these really good operational hackers who can really like chain existing vulnerabilities together. But what happens is that OK you get this researcher who can come up with this vulnerability.  And then they themselves will not be able to put together. Oh, and the reason why this is really bad is that I can do this chain where you know this exploit chain that gets me somewhere else. So what? This ends up happening, you know, in, in, in state. You know apt is where they are the ones who are able to do this. But us we are mortals are not able to piece together the real consequence of any vulnerability that comes our way. So it looks like a low C VSS may in fact be really really big deal. So what I'm hopeful for is that with these AI tools we'll be able to do more.  Automated exploit chaining.  In a way that makes it more obvious which vulnerabilities really matter and which ones are just kind of like you can't actually get that like log 4 J seemed really bad, didn't actually turn out to be a big deal. | | |
|  |  |
|  |  |
|  |  |
|  |  | P22 |  | we were wondering whether to suggest the US federal government's approach of an espon, you know, software bill of materials.  And that the guys who?  Of operational it guys were saying can be stupid. Yeah, most most sensible organisation have got probably like at least 50 to 100 different suppliers built up in their system.  You having an S form would just add to the complication. I mean it wouldn't do anything because you know you've got to keep up with update cycles of each of them.  And even if it's BeenVerified at Level 3.  By the time it goes to level 3.109, do you have to re verify it? | | |
|  |  |
|  |  | P3 |  | But then there's sort of issues around sort of use of cyber threat intelligence or threat intelligence.  Basically, in this space, right?  So there's a whole issue around, yeah. | | |
|  |  | P3 |  | You know, if you if you have an organizations that has some sort of risk management program, risk assessment, governance, risk and compliance program, a major component of that will be the sort of application of cyber threat intelligence of different sorts threaten to other. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 17 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | So you know we need sort of technologies that are appropriate and robust, right to to defending against these acts that sort of exists within a an architecture that's sort of tolerant to the failures of these things from an adversarial point of view.  And so that, you know, we have like this.  So there's this idea of having guardrails.  So, so, so, so.  So they they kind of like uh, analog or whatever kind of measures in place to.  So if you have some sort of AI based system, for example that's doing control, you know what you wanna do is monitor that and then if it looks like it's going in a in a bad direction.  So to have some sort of guardrails to kind of, you know, detect that it's going in that way and sort of have to controls to stop the system doing something bad for nuclear safety view, so architectures, best practices, standards guidance, right, we need all of that.  I think I mentioned that before. | | |
|  |  |
|  |  |
|  | | | | | | |
| **AI to Create Software** |  | | | | | |
|
|  |  | P12 |  | And I also think that the more this is going back to AIA little bit and the more kind of way that I think about AI, when I look at AII really see this is almost like the way I would look at like a compiler where like we had assembly, right. And then there's this compiler that's interposed between you and the actual assembly code.  And as you work your way up that stock, you know with Python I don't even know what's happening at the C++ binary layer, let alone what's happening assembly. And now I think like AI and generative AI in particular has really interposed at a level above where, you know, I know people who are using, you know, llms to generate Python. And that's just another layer of interposition. And I think that as AI interposes more and more in that stack, the more it becomes difficult to discern what's actually happening. And I think to this question, yeah, that does potentially make it harder to discern whether something was.  Misconfiguration or yeah, an an attack. | | |
|  |  |
|  | | | | | | |
| **AI to Help Manage System Complexity** |  | | | | | |
|
|  |  | P14 |  | Anticipation sensing, interpreting the data. A dashboard use of dashboards. | | |
|  |  | P14 |  | As more systems become connected.  There is greater complexity. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 18 of 316 |  |
|  | | | | | | |
|  |  | P17 |  | I think the likes of.  AI is a productivity tool.  Could be used to bridge the gaps in skills, but also the management of knowledge in terms of well, you might only be able to focus, you might be. There's no disrespect to any human being, but you know you might be a very simple person and that you know you're just there to do your job. And and this is the kind of bandwidth that you hold in terms of what you want to do and anything outside of that in terms of additional skills and whatnot is probably it's not even that you can't comprehend it. It's just you don't even don't want to or you can't. It doesn't. It doesn't. Doesn't really make a difference really.  And so you need that awareness and that expansion you need to sort of take on because technology is growing, it's evolving. So you need individuals to follow that curve, right? | | |
|  |  |
|  |  | P17 |  | But we can't because we're human. We're only, you know, we do what we do because we're born to do it that way. Our brains and our anatomy is built that way. And so either is or it isn't. And unfortunately, I think there's more of the isn't than there is in to some degree. And that's fine. That's absolutely fine because that's part of being human life is, you know, that's what it is, but I think.  You could leverage the likes of AI to help like things like workflow processes and a little bit of automation so you know if you could fill the gaps into tail telling someone you know you don't need to worry about this. This is what you need to do. Or if you complete this task and then this task then this will remediate the finding that we found then that could be used to help you know plug the gap slightly with with this expansion in technology and how sophisticated it can become. | | |
|  |  |
|  |  | P19 |  | It could be that that this is where with trained systems it and it given enough experience.  Of maybe actually relatively rare in time.  If you build up enough experience, you could get automated systems.  It could help to just send you. | | |
|  |  | P19 |  | This might be your future use of these so called AI.  And these these could be in the past have Prince, that's been thought to be very expensive, but maybe with technology.  But shooting these kind of systems might be more you not really feasible in the future.  This is the sort of dark.  Trace, whatever kind of thing.  Looking at what's happening, yes, saying yes, I think yes, but build it building on patterns that have been observed from the from previous incidents.  Yes, yes, this this is a deliberate time is something that's been accidental. | | |
|  |  |
|  |  | P7 |  | coming back to the to the AI is the is a sort of intelligence that we need to embed in those in those systems.  And and you know the.  I mean, it's still early days, but you know if you want to the to the complexity mix, the fact that a you might have to do learning over resource constrained environments, B you have to integrate data from diverse sources that looks different, blah blah blah they cannot, it cannot readily be integrated into a coherent model it it makes this an even more complex complicated space. | | |
|  |  |
|  |  | P7 |  | And the second I would say.  Technological sort of breakthrough that needs to happen is what sort of support do we need from the physical infrastructure in order to be able to do this. So in order to be able to do instrumentation in order to be able to do monitoring in order to be able to do data capture in order to be able to then ultimately run our our nice algorithms where AI will tell us what's what's right and what's wrong.  Where where this functionality comes from, if you ask me, it should come from the network, not least because it's it's it's impossible to to to try and instrument everything. All devices across all vendors, all all types of devices. So the network has the opportunity to act as the the natural aggregator that that, that it actually is and and offer this as a service to the connected to the connected end systems. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 19 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **AI Truth - Fiction** |  | | | | | |
|
|  |  | P10 |  | Yes, yeah. And deliberately polluted data as well. I don't think that's come up in, in your work. So that's another way to. That's another way to kind of mess with systems if you're if you're, if you're a hostile actor, you might just deliberately pollute a data set and you can do that remote. And then in a sense, because it's, you know, AAI is not a thing, it's stupid, would kind of carry on doing this. I'm also we're looking at a nice kind of far horizon here. And I think this is going to happen within, given this, the pace of change. | | |
|  |  |
|  |  | P10 |  | Swiftly, but sort of, you know, AI, data sets and material. It's what, when when does the tipping point come? What it's learning from is other AI generators material. Yes. So it's kind of AI training, AI learning, so that that sort of that sort of thing. | | |
|  |  | P10 |  | Yeah, you start to, you start needing a way of tagging things as created by AI 'cause. Otherwise it's just AI learning from AI and it's not. | | |
|  |  | P10 |  | Exactly. Yeah, it's that sort of photocopy of a photocopy of a photocopy and and the the the degrade, the degradation or the degrading is is is going to be interesting to see what happens when I hope it's not keyed into anything critical. | | |
|  |  | P11 |  | I would go further and say it shouldn't matter whether it's malicious action or failure.  In your first response and if you go to a computer security.  Manual and it tells you that there's a computer security incident response procedure and the first node says determine you have an computer security incident.  I will immediately reject it because in many, many cases where you have a complex only partially observable environment, particularly an industrial one.  The first thing you observe is that it isn't working the way it did earlier, and it's probably what that maintenance tech did, or some idiot on the control panel or something's broken.  And it's about 48 hours later when you've exhausted every other possibility that you might say oh. | | |
|  |  |
|  |  | P11 |  | We were to get some other people in.  So exactly to your point, no, I I'm sorry. I thought that was that was a given. | | |
|  |  | P11 |  | It's. Yeah. Well, it is a major issue, but it isn't yet resolved the other, so I'll just return to the point that I was going to make earlier because I was a little bit rude about my safety colleagues thinking that everything is about sort of random failures of pin joints with sheer bolts and things.  I think the problem I have with my security colleagues is that too much is about defending the network and the network attached assets to computer based systems. The software and you can actually have a conversation with.  Then for all forever for a day, and never once did they say. But what does this place actually do? | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 20 of 316 |  |
|  | | | | | | |
|  |  | P12 |  | Signed off on this right and I think when you're, you know, trying to like put that on, you know, oh, the White House is iCloud account is getting off on this. Then you're in a world where deepfakes don't seem so scary to me. Maybe. But maybe I over estimate people's.  So, you know, belief in how these things work because again, this is all predicated on people actually believing the cryptography works. And you know, you don't even think vaccines work. I don't think you can probably be expected to believe the cryptography works. It's even more abstract. So, you know, I don't know. I don't know. | | |
|  |  |
|  |  | P12 |  | 'Cause you could be a deep fake of Charles and I actually have no way of seeing that this was generated by. | | |
|  |  | P12 |  | And the thing that you're forwarding, I can't look at that metadata and then see a signature and in that signature see, this was generated by the White House. So if I and my signal group chat get a video and it's like Joe Biden being like, dear Americans, please don't panic. But like, there is nuclear bomb coming. Whatever. You know, I might be like and and unless I can tap on that and see that there's some, you know, kind of programmatic way of really verifying that this was generated by the White House then yeah, I I I think that that's where we get into problems but again.  Really do see that as more of like a usable security problem than as an AI problem per SE. And we have always had this issue before AI. We have still had this authentication issue when it came to authorities and HTTPS again helps a lot with like me and Microsoft doesn't help with media. | | |
|  |  |
|  |  | P12 |  | Yeah. So I can't even like look at your participants, you know profile or anything. So again, it's stuff like this where I see this is like not so much an AI problem and more design problem that honestly people have been punting on for like 20 years anyway, which is big end to end authentication and like look, we have signal Messenger or WhatsApp or whatever like honestly.  We're kind of does this in a way. I think that what gets scary is where people are forwarding stuff. | | |
|  |  |
|  |  | P12 |  | So you're so you're you're thinking of handling the deep? Yes, it wouldn't. It wouldn't deal with certain situations, but it would allow me to send you a photo and you to say yes. I believe that was the photo that that Charles produced. Yes. Yes. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 21 of 316 |  |
|  | | | | | | |
|  |  | P12 |  | There are two sides to this. The first side. Yeah, you know, this is something that could exacerbate panic and misinformation. That's not really my area. It does seem to me like we as a security community for a long time have had cryptographic tools for dealing with this kind of situation in the form of, like cryptographic signatures and stuff. And I do feel that there were, I mean, there are voices on many sides because the EFF is always kind of these days, in my personal opinion, kind of being really useless or counterproductive. But.  There have been, you know, a lot of civil society organisations that were like, hey, you know, you should consider having some kind of cryptographic scheme, you know, in your national identity card, to allow people to sign content. And I also think that it's within, you know, Apple's power to have some. Yeah, I think even maybe because they use pass keys now. So maybe web authent even allows you some kind of signing key. But to allow, you know, your device to sign.  Contents so that you can say, well, I I you know.  Like there's some evidence that I captured this or whatever, and when the absence of that signature that I can, whatever, you know, those solutions do exist. So whenever I hear about this aid, fake stuff like, you know, first of all, I agree with you a bit generous to AI. But but I do think 5 to 10 years it's reasonable to expect that perhaps this stuff will get better. My question is where are the companies on this, you know, producing kind of cryptographic schemes to, you know, and. And I do think we'll probably just someday see an apple.  Saying hey, we we we allow this now with your iCloud iCloud is the only fully verified authenticated way. So you have to get an iPhone and actually you can't even check the signature unless you have an Apple device. If you have something like but whatever you know honestly that is better than the world we live in today. So I would I would I would salute that and say OK you know deep fix kind of partially solved there and apple and trenches there they're monopoly even more but yeah that's kind of how I think about that stuff. I I I will say though I could really be missing something in AI and often when I talk to people about AI and here in the Bay there are a lot of people who really.  AI and Agii often feel like I'm missing something.  So I don't know if this is like crypto where I was, I was right, or if I if this is another thing where like I am really missing something. So we'll see you know. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  | P13 |  | People's behaviour is changed by things that they read that are not necessarily true.  And so you can imagine that those kinds of things could be more manipulated by those technologies more easily.  Just because they're potentially more convincing.  Well, well, exactly. Exactly. | | |
|  |  | P13 |  | If you want to know whether a particular drug treatments is effective or not.  You really need to do randomised control trial with a large sample of people and have it published in a peer review journal and then you can trust that.  Then there are all sorts of shades of this in between.  From what we talked about.  From just simply Googling something and somebody says something, well, there's a truth they're not true. Who knows? But that again, I think is.  Down to the population and.  Being educated to understand.  How to distinguish fact from fiction? Essentially, do these technologies make it harder? Yeah, probably they do. | | |
|  |  |
|  |  | P13 |  | If you think about the relationship between patients and healthcare professionals, it's obviously one built on trust.  I don't think I see that being maintained.  Though of course I painted a picture earlier of increasing.  Let's call it algorithmic healthcare for want to the better word. And so your scenarios would fit with that. So there is potential that that could happen every we move in that direction.  I mean it. It's also possible that you see increasing sources of the misinformation.  And you see this, I think already not, not particularly motivated by AI, but it's the same kind of thing in terms of vaccine hesitancy.  Where actually. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 22 of 316 |  |
|  | | | | | | |
|  |  | P14 |  | Absolutely. So I I experimented with this electromagnetic project. I experimented with asking.  To do a piece telling me what's significant about the electromagnetic environment, and actually it did a rather good job, but because I was doing it for the first time, I said to my son, who's a barrister, I've heard about this, it's called hallucination. You know, where where it makes stuff up.  You are. You're an expert in planning law. Ask this chat gpta question and he asked a very simple question, which was?  Our local authorities allowed to do this under this law.  He knew the answer was no ChatGPT said. Yes. Not only did it say yes, it quoted chapter and verse the law that allowed that, and it did it in a nanosecond.  The chapter and verse and it was a it was a real law, but the chapters and the verses were complete. Make believe it had just made it up.  In beautiful legalese language.  Total \*\*\*\*\*\*\*\*. | | |
|  |  |
|  |  |
|  |  | P14 |  | But utterly convincing.  And beautifully, all in a nanosecond.  I was amazed, yeah. | | |
|  |  | P15 |  | And | | |
|  |  | P15 |  | Definitely like if you're.  If you're looking at data to try and understand what's going on in a major incident, I mean back in the day, people would look at Twitter and see what people were saying. If if sort of hypothetically like that that exists in that context. But half of that stuff is misinformation or is about something else or you're using some kind of tool to not like APC going in and looking and saying, oh, I've just seen this, this person's reported this or that person's reported that or.  I know they're analysing the 300 calls that will come into it to make a control room, to understand, OK, what are the key bits of data that we can get from that if those things are being fed by misinformation and disinformation, then that could lead you to.  Deploying the wrong kind of resources in the wrong quantity to the wrong place. They could be at risk.  And therefore you would be delaying. You would either be running the wrong response because you think a different kind of incident is happening. I I you think a firearms incident is happening rather than a bomb.  With with screws and bullets in it that made people look like they had firearms injuries.  It is a firearms instant because my friend's just been shot. They haven't been shot. It was because of the.  Shrapnel and stuff in the in the bomb. | | |
|  |  |
|  |  |
|  |  | P16 |  | Exactly. Yeah. I mean, I just like, I mean, you read probably like everyone else, this poor fellow, poor chap in Hong Kong that was lured. I don't if you've seen it, it was lured into a zoom call with six other people from his company. He was working in Hong Kong. I mean, he's working in Hong Kong and his bosses were in the UK. So he was summoned to a zoom call with six people requesting him to wire $25 million to an accounting in the UK.  And actually, none of those people were real. They were all AIS, and he was actually.  Manipulated into wiring this massive.  Amount of money, but only by AII mean. No one ever so. So yeah, it's going to be really.  Complicated and tough to to verify the authenticity of someone now more and more. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 23 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | The all the employees to help them.  Understand the new AI threats. So those I was just reading before Oracle the the new report by the.  Your National cybersecurity centre.  Where on AI threat and who's going to make the most use of it. And they were explaining that we're going to have to train people to understand that now any e-mail that you receive from anyone can be coming from an AI and not from a human.  Still be very, very persuasive and be be perfectly. | | |
|  |  |
|  |  | P18 |  | So we're nuclear, I guess the the consequence of that is that we in nuclear, we put a lot of emphasis on lessons learned.  If it's, if you're. If you're unable to detect the reasons why something has failed, then it's very difficult to do. You know the lessons learned and you know that the more complex the technology, I think the less able you will be able to understand why why it's failed. So why AI is given a reason, an answer out. And for instance, which is, you know, is obviously going to happen.  Yeah. So it's it and there's no way of doing that in many cases, you know certainly for kind of.  Generic models then?  Yeah, it's kind of that, that I don't know whether this is helpful, but that that.  It suggests that you need to have that corroboration approach. You know the AI is saying a how are we going to corroborate that and that that doesn't go a, A is not magic. It still needs that corroboration that we've always done. You know, if something's important, you don't just take one piece of evidence and say, look, it says there that it's important and then accept that there seems to be a kind of again it goes to mindset with people.  No, it's AI that could it, so it must be true, you know? Yeah. | | |
|  |  |
|  |  |
|  |  | P19 |  | But the trouble is the media likes to from board is kind of fears and I I I don't think it it makes I don't think these AI systems.  I think they don't make the need for resilience anymore.  This Emily, don't make it.  Any lights?  So you see them just as increased computing really well people just creating this, yes.  I mean they, they mean that there's even more data.  Course, yeah, even more data that's been stored.  And and the more data that's stored, the more the haps important is to protect it. | | |
|  |  |
|  |  | P19 |  | Yes, umm, I think it's very unfortunate that.  Popular media.  From watching the notion that the AI is something perhaps more than it than it actually is, yeah, I I think that the I actually just said once the computing, it's work computers got to, yeah, the sheer polar machines, the sheer magnitude of data that can be controlled over tremendously capable communication networks.  It just means advanced computing, and then there's too much scaremongering around AI if you if you talked to, I think many, many EI, the experts would probably readily see that that that AI systems got no semblance of Human seems.  Yeah, at all. | | |
|  |  |
|  |  | P20 |  | The processes that involved around data Cleek cleaning and the elimination of bias in data.  From what little I know of it, they don't appear to be particularly robust.  Their subjective processes in themselves.  So I think the trend is that that's going to be increasingly problematic as we have more and more algorithms which rely on data sets. So you know we've we've seen this already with ChatGPT and them having lawsuits against them from from data that they probably have harvested and used to train their data illegally.  Actually, that's subject to court cases and court proceedings, but.  You know this access to data access to good data.  Access to data that is done in a way that's you know that accords with privacy and copyright and commercial and intellectual property.  Rights, I think, is a is a huge, huge problem in terms of it being a trend. I think it's definitely a trend and that's going to become more, more and more contested and problematic. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 24 of 316 |  |
|  | | | | | | |
|  |  | P20 |  | There's just as much violence and and misinformation and disinformation and extremism online as there is there ever was probably, in my view, I don't know whether I'm statistically accurate in saying that, but it certainly seems that way. So yeah, I think the trend is in a bad direction. And in terms of data bias and integrity, I think that that's a big problem. I'm one of the things I'm doing at the moment on the AI security stuff, is looking at data poisoning as a method for, for manipulation.  Predation of of AI and algorithmic systems and and the data they're using. It seems to me a pretty.  Prevalent form of malign activity, one that's growing in sophistication.  I think I've been sceptical about this idea that you can ever have completely unbiased data sets, but data reflects the bias that's in society.  But it can also be very consciously manipulated by malign actors in ways that will lead AI to not function in the way that's intended intended to so.  I think I'm interested in.  You know, it's a disinformation side also the the.  The growing sophistication of data poisoning, interference with the integrity of data. | | |
|  |  |
|  |  |
|  |  | P20 |  | Yeah, there's the you know, obviously if you if you spread misinformation and disinformation, you're kind of injecting bias into the world, aren't you? But I mean they I guess at least I've thought about them as separate issues. Yeah. I mean, look, I think that technology means that we're becoming ever more capable at at developing and disseminating disinformation deliberate, deliberately spread, spread misinformation, misinformation.  And that people are absorbing a lot of misinformation, which.  You know, might not be spread deliberately, but which is just out there.  So I think the capabilities to do that are are becoming more sophisticated.  Obviously we're trying to regulate that, but it's difficult because it means rely on being reliant on.  The companies where the disinformation is spreading.  So that's Twitter or Facebook or Tiktok, and we don't have regulatory control to sufficient degree of those companies. Companies, in my view. One example is this whole new post, Christchurch attack, Christchurch call about eliminating extremism online, which followed the live streaming of the attacks against mosques in Christchurch in New Zealand. And it was like, Oh yeah, you know, sure, we'll have a big lobbying effort to get these companies to remove this kind of information, but, you know.  Has it really changed anything? | | |
|  |  |
|  |  |
|  |  | P20 |  | Now, yeah, it's. It's a fascinating thing. I mean, I think I'd.  Yeah, I think the way you phrased it, there's a couple of things that may need separating out. You've got the miss information on on the one side and then you mentioned another aspect that you.  Price data? Yeah. So, I mean, I think. | | |
|  |  | P21 |  | Yeah, I think AI certainly perceived as a tool for cyber criminals to launch more targeted.  And highly individualised fishing attempts, for example, in a in a faster way. Also that it expands their ability to target areas that were previously perhaps unlikely to be targeted, for example.  ChatGPT as a large language models being perceived as an opportunity for cyber criminals to expand in areas where they've previously not been able to speak the language. Japan being a prime example.  And we were very culturally sensitive and complex language.  And previously Google Translate for example just wouldn't wouldn't translate to an extent that that would make for a believable phishing e-mail. Whereas with increasing ability of large language models to.  Mirror that language, including cultural references and cultural context. That sort of the fear that that would have mean open up new.  Pockets effectively for sagaminals, I think that's.  And I think on the other hand, the opportunities for AI in a cybersecurity context are often overlooked in terms of vulnerability detection, patching and so on. AI can also work as an enabler for cybersecurity for the good side, so to speak. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 25 of 316 |  |
|  | | | | | | |
|  |  | P22 |  | Mm hmm, but to me it seems this seems an application with all with very much plus side, whereas things like recruitment using AI seems to me to have very much negative side because it locks in historical patterns and you know, as a scientific woman, you know, I'm not happy with being recruited on, you know, criteria for recruiting scientific women in the 60s, you know, which is where out of data originates whereas, you know, if you're tracking faults, you know, having a historic track is actually what you want.  And so please do AI strengths rather than locking in weaknesses. | | |
|  |  |
|  |  | P22 |  | Yeah. Still, mm hmm. Yeah. So you'll get some, you'll get some false flags if you use AI to monitor our failures. Yeah, so people can be wrong too. | | |
|  |  | P23 |  | It's certainly a big concern and one of the one of the you.  So there's a lot of obvious things to say, but what what I would be worried about is that once deep fakes and misinformation don't have to be very good to work.  We're not that discriminate in our consumption of information.  We don't look closely. I'm.  So even a not so great deep fake can be efficacious, and there's very interesting work going on at xxxxx.  I have a colleague who is working on the kind of end to end. I'm.  A watermark for cameras and other media.  So you can you know when you get the New York Times and there's a photo in it, you will be able to say that photo has been edited. | | |
|  |  |
|  |  | P23 |  | It's it's a path dependence problem.  When we passed security breach laws in the US, are threat model was identity theft? | | |
|  |  | P23 |  | Can't remember what that's called, but I I think I I think the day is not far away where we're gonna need, you know, politicians and other important people to use technologies in their communications to prove that it is that it has integrity. | | |
|  |  | P23 |  | And but there are newer security breach disclosure regimes that require disclosure of any material Security event.  This is our security and Exchange Commission requires this, but then they kind of trick is. | | |
|  |  | P23 |  | Any any public company, so any publicly traded company has to disclose material security events.  It's kind the problem is, is that material, umm, a company can make an argument that even losing $10 million is immaterial or even 100, right?  If if you're apple and someone steals $100 million from you.  Like you're like, literally a $2 trillion entity. | | |
|  |  | P23 |  | It's already problem for businesses that are being swindled through deep fake videos and calls, and we don't know it because that's secret like it's not, it's not considered a security breach.  So no one has to admit that they were swindled for $100,000 or whatever. | | |
|  |  | P23 |  | It might not be material and so.  So we have, we still haven't figured this out of how to kind of get this balance right. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 26 of 316 |  |
|  | | | | | | |
|  |  | P23 |  | Why is it that that you don't that particular form of of fraud doesn't have to be reported cause is it you know, whereas some other sorts do?  I'll think about. | | |
|  |  | P23 |  | Maybe it's been cropped, you know, but you can say for sure that it hasn't been perturbed for its content. | | |
|  |  | P4 |  | Yeah, I mean I I have seen ambiguous.  I have seen discussions on contracts around certain things and is this partner doing this or doing that in my particular field?  But usually that's not malicious.  There's just people not reading things properly, but in this example, which is more, which is more scientific rather than commercial, it was literally intentional because these people that were so experienced at with with the software and the requirements and they had so many bad experiences that they literally were very defensive when, when, when their own specs. | | |
|  |  |
|  |  | P4 |  | They were literally exploiting the fact that people were perhaps being ambiguous, but not realizing that they were being intentionally ambiguous with their sort of specs in order to bite some to to sort of buy some grease because the system changes in in, in in the future, it's not something, it's not something I've seen anywhere else.  Uh, But what I would say is that these people, I mean, I mean flight nomics folks have been writing software since since the mid 60s.  They are very.  I mean, I've I've literally written a paper about this.  My first ever academic paper was about requirements for, for, for.  For these sorts of people, they're very, very, very seasoned people at software engineering.  But even though they were preceded that as a sort of discipline, but yes. | | |
|  |  |
|  |  | P4 |  | They could say, well, you know, we we could relax that, but that other requirement over there that you said you couldn't address, you'd really need that to be done in order to sort of to sort of to sort of do that.  So it'd be very, very canny about. | | |
|  |  | P4 |  | So this would, I guess be an example from space cause I I wouldn't call space or critical infrastructure, but I used to do some work in in that area, but I want once worked on a project I once worked on a team with with flight dynamics engineers and they were they they would write software for controlling the orbit and the attitude of of a spacecraft and they do it for all sorts of missions and they've they would they were very adept at writing requirements because they had to for other systems but they would they would they.  Would sometimes want services from other parts of the ground segment, specifically mission systems and the and because of the way the contracting stuff worked, it was always very hard for them to to get eddies sort of feedback.  So what they they developed this ability to write requirements knowing that they wouldn't be interpreted properly and knew that they would be able to if they wanted, they could take a strict interpretation of the performance of that particular requirement.  But such that when's the other people in the ground said and found out about it? | | |
|  |  |
|  |  |
|  |  | P5 |  | It's gonna absolutely become a much bigger problem, I think so, yes, I would absolutely be focused on one of those, that technology.  With the trust issue in the Truth ground truth. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 27 of 316 |  |
|  | | | | | | |
|  |  | P5 |  | It hasn't been that much, but I see that trend coming towards me that way.  Absolutely.  Umm, you know, we talk a lot in the past about an operator sitting at all of his screens or her screens and looking at the data.  And do you trust the data or not?  How would you know if it was right or wrong, you know?  And So what are those other systems that may not be digital that you think you do trust, which are analog, that you can compare at least or something like that and with all the deep fakes with the AI, with all these things that are just coming on the ICT side of things, it's gonna work its way into the operational technology.  It's gonna work its way into the nuclear world. | | |
|  |  |
|  |  | P7 |  | So I think that's the that's potentially a very big problem for for all sorts of sectors and it's and it's similar to you know potentially quantum computing that might be the other technology that's down your list, right, can can can be used for good, can be used for, for for bad to, you know, weaponize an adversary. Yes, I think that's potentially a very big area and and a very big problem because now you know if you are on the defensive.  You not only need to have you know AI to, to defence, to defend against.  Things happening, but also to be able to defend against deception, which is, you know, a very yeah.  Yes, a very complicated.  Very complicated thing.  Engineering that is quite quite often involved in cyberattacks.  Again, can be weaponized by by AI.  You know, imagine, imagine how people are being fished, you know, through through, through fishing attacks, without being so intelligent. But still people fall, victims of it. Imagine if it's, if it's even more more weaponized. So, yeah, I think I think that's a big problem. | | |
|  |  |
|  |  |
|  |  | P7 |  | That's also a big problem.  Complexity in general is a big problem.  It's inevitable that systems become more complex.  But then when they do it's it's harder to it's harder to contain. It's harder to understand. It's it's harder to debug when when things when things go wrong.  When when it comes, when it comes to people being able to distinguish what is malicious versus what, what is an accident?  The obvious answer is yes, but I'm not sure this is the sort of more, more critical point, so long as you know if the consequence is the same.  You need to revert the consequence, right? That's the sort of first first thing that you need to do.  Whether it comes from a from a deliberate action or or from an accident might be a sort of second level analysis. It might not but but but. But it also might, but complexity is is more general. | | |
|  |  |
|  |  |
|  |  | P8 |  | Yes, I mean that you know, like they said today. So it isn't it like this guy in Hong Kong.  The finest guy. Have you heard of the story like that? He had his own call and then he thought it. He was talking to his real colleagues. But the real faces were was he called again and of like an AI technology product trade? Yeah.  A lot of people work with trust, especially, you know, we know it from human factors and psychoso by looking at faces, I think.  And other people know the risk in terms of buying some. I sent you an e-mail, but when I'm speaking to you, is this really you or is this someone pretending to be you? I see this being a risk, yes. | | |
|  |  |
|  |  | P8 |  | No, it's just me. I just love it. Look like Brad Pitt. But this just me. Yeah, but really, did I think this is very underresearched. We know nothing about it that we miss SH FP people. We have no evidence how this would impact. So this is yeah, it is very scary in my view. Yeah. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 28 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Attacks Different for OT** |  | | | | | |
|
|  |  | P7 |  | There are systems that run bespoke hardware bespoke software, so you know it's less. I suppose it's less easy to to just buy your your usual denial of service credits and and and just just fire an attack to A to a power plant. So the consequence of this is that the the potentially the attacks that we're going to see there have very specific signatures that we don't know off and and and it's hard, it's harder to harder to create.  Public knowledge of right? | | |
|  |  |
|  | | | | | | |
| **Better Identification of Attackers** |  | | | | | |
|
|  |  | P21 |  | I see that as a as a trend.  I actually think in sort of an an offensive side of the term. So we've become relatively.  We've become better at doing technical attribution on identifying who's behind things, and we've also seen more public attribution of cyber operations. And then sometimes you have in case of a ransomware, the attacker more or less makes known who they are, at least in terms of an affiliation of an anonymous group. So in these instances I would say you can distinguish between accident and malicious.  Actor, that sort of more on the cybersecurity front, I'd be. I think it's harder on the disinformation front to distinguish between that. | | |
|  |  |
|  | | | | | | |
| **Black Box** |  | | | | | |
|
|  |  | P12 |  | , when I look at AII really see this is almost like the way I would look at like a compiler where like we had assembly, right. And then there's this compiler that's interposed between you and the actual assembly code.  And as you work your way up that stock, you know with Python I don't even know what's happening at the C++ binary layer, let alone what's happening assembly. And now I think like AI and generative AI in particular has really interposed at a level above where, you know, I know people who are using, you know, llms to generate Python. And that's just another layer of interposition. And I think that as AI interposes more and more in that stack, the more it becomes difficult to discern what's actually happening. And I think to this question, yeah, that does potentially make it harder to discern whether something was.  Misconfiguration or yeah, an an attack. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 29 of 316 |  |
|  | | | | | | |
|  |  | P14 |  | What's really interesting, especially talking about the cybersecurity behaviours piece, is how people will say to me, of course, AI machine learning might be able to help, but also there are real concerns.  First and foremost, one that you'll get more than most is just the trust question. So, so much AI and machine learning goes on inside the black box.  For the ordinary lay user customer client stakeholder.  Are they going to buy this if they can't have it spelt out in sufficient detail to make them feel reassured, this is going to deliver a robust and reliable service that's explicable and there's, you know.  In a separate life, I I I found it a early stage company back in 2014 which was using machine learning to help video analytics and one of the issues there was. | | |
|  |  |
|  |  | P14 |  | Us to an address which took us to an occupant who had the same appearance as that person, and when we opened the cupboard we found the bag of swag and therefore when you join, that's that, that that's actually dealing with human judgement rather than what the hell it is that the machine learning algorithms are doing. But when you're dealing with how cybersecurity is going to be delivered by artificial intelligence.  Particularly if.  And this is another of the concerns being raised by the experts I speak to.  And then corrupt the learning data. So actually the machine's giving the wrong information. | | |
|  |  |
|  |  | P14 |  | In particular, to help law enforcement, and you know, if you.  Bringing someone to court based on the video analytics.  The judge might want, and the jury might want to hear an expert stand up and explain.  How they can be confident in?  That capability.  And frankly, what I you could do your best to explain it, but frankly one of the most.  Reliable options would be to say the human has been in the loop. You need to question the human who reached a judgement based on the data that he or she was presented with, and to then explain the steps they took so you know the person in this video looks very similar to me to be the person who appeared out of the bank with a bag of swag on their back.  I was able to track that person to a car. | | |
|  |  |
|  |  | P18 |  | You know AI so difficult because it's complex, you know, at the end of the day, it's only doing statistics, but but you know it's it's they're very difficult to understand what it's doing because of the complexity of how it does it and the lack of understanding you can get from from that. | | |
|  |  | P23 |  | There's like there are very very basic things like her.  Have you can have you allowed your control infrastructure to be connected to an Internet?  Resource like the most basic A that are not fully ironed out and the attacks against these infrastructures tend to be really basic stuff, not quantum stuff.  I'm gonna find you on LinkedIn and I'm gonna send you an email and ask you to log into the control site or the other.  So it it we really are at at our infancy and and and one of the questions, one of the great questions out there is why why haven't we had a disaster?  Umm the and there is some speculation, you know, like why haven't we had a dam loose control and kill 1000 people and the there is speculation that in fact many of these institutions do not but the you know the larger ones have not connected their control to the Internet and and so on yeah another reason is that many of the infrastructures are quite old and that and the way makes them difficult to attack because no one knows I mean I mean I know Web programming languages but I do not know Fortran and so on. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 30 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Cannot Measure Cybersecurity** |  | | | | | |
|
|  |  | P7 |  | So if you look at some, if you look at.  Different standards. You know, I'm thinking of 6483.  The calves that you see from NCSC and and other bodies cyber assessment frameworks.  And and and other standards when they touch cybersecurity, their their guidelines are very generic.  Very, very, you know qualitative, you know they will tell you you know, if you have systems speaking to each other then communication better be encrypted. But this is as far as as they as they will go. | | |
|  |  |
|  |  | P7 |  | And and quite a lot of quite a lot of processes and systems are are based around building a safety case for them, and if you have a safety case then then you can do things. You can patch software, you can. If you have a safety case for it.  The same thing doesn't exist for cyber.  Not least because.  We don't really know how to measure it. | | |
|  |  | P7 |  | How much you know how much of our, let's say, telecoms network? No, not not to to come to how much of our telecoms network need to be?  Survivable if you like.  In the event of a of of a global of of an attack from a from a foreign state actor.  To maintain. To maintain safety, you know, it's all all these things are not quantified. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 31 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Cascading effects** |  | | | | | |
|
|  |  | P10 |  | Yeah, that that is that is quite catastrophic. I mean, yeah, I mean that's certainly possible. But I think the sort of the traffic cascade of one, you know one small item, one small you know error you know and you can tell I'm a classicist. Now I'm thinking you know, it's just that the hamatia it's just one, one sort of tragic flaw and then which might be sort of trusting in the system. But I'm also thinking, I mean this, this needn't be a hostile.  The hostile attack, the government Social Security strategy, for example, really focuses on on the the vulnerability to to external threats, and I think downplays the role of what they used to call insider threat. But, you know, just just, just \*\*\*\*\*\*\*\*\* like me, you know, making a mistake. But I also I kind of want to see the natural world as a, as a vector for risk in in, in this. So we just get horrendous flooding.  And or you know that that that takes out that takes out this, that takes out that and therefore, you know leads to this.  I was this is this is a sidebar anecdote, but I was her family who lived down in the West Country and they were built. They are still building Hinkley Point. The new nuclear reactor, you know, Somerset levels. It floods with extreme regularity and the the planners were were reassuring everyone that you know it was was designed to, you know, built to design this much level of sea level and this much salination it was all perfectly designed. And then someone said.  How? How is anyone gonna get to work? You know, you have this you. Yes.  It's just the simple things. It's it's it's fine. Yes, that the infrastructure, the architecture will do this. But however, people who you know man the pumps and do this and run the health, how are they getting to work? Are you ensuring everyone with a dinghy so they can? It's those, it's that sort of implication of of complicated. That's the messy stuff and that's why I think narratives are so important for doing this kind of work because you need to think about the people and the.  And all those, you know how? What do they have for breakfast? How do they get for lunch? What do they care about what keeps them at home? What motivates them to forward that e-mail to, to, to work those? Those sorts of things? Yeah. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  | P10 |  | There's sometime in the future and I I don't know, this is just 'cause. It's on my mind from conversations we've been have been having and and sort of the work I'm doing. But there's there's again this is sort of database, there's evidence just that people.  Kind of trust in their organisational.  Sort of protections. You know, they might not trust at home, but on the work. I think if they work for government or work in, you know, a a critical.  Part of of of the Society or the financial sector or health or whatever, and so if they get a dodgy e-mail, they'll fall. They won't open at home and they won't open up on their phone because it looks, you know, they've used their intelligence. So they'll forward it to work and they'll open it at work because they believe, you know, that everything will protect them there and that that there's there's, you know, we know that people do this. And if that is kind of terrifying and that's the sort of someone who who thinks they're, you know, doing the right thing and and sort of almost trusting in the systems that we've said are in place.  And and therefore, you know sort of that that sort of cascading effect. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 32 of 316 |  |
|  | | | | | | |
|  |  | P10 |  | That Tropic cascade we've already been talking about, yeah, absolutely, absolutely. And yeah, the interconnectedness around supply chains, but, but particularly the the sort of the sort of cyber connection here is is, is, is critical, absolutely.  The other thing that might be worth mentioning is this is sort of got a natural world agricultural metaphor to it as well. So I'm just sort of doing GCSE sort of history and looking at, you know, the American Dust Bowl and and the problems with monocultures.  We the the the risk of monoculture in security subsecurity in particular is if everyone, let's say, everything government is run on Microsoft because they're very good and you know, I've no criticism of Microsoft. But if it's a monoculture, you get one floor. Great, you've got one floor and it gets, you know, it kind of goes across the piece and there's again just looking at good data. Microsoft, if you if I am a malicious person and I want to you know create a but I'm I'm going to target Microsoft because it is.  It it is buggy and it's going to have, I'm going to get my greatest bang for my buck. I'm not going to be trying to work on something. What is it that submarines run on? You know something that's really archaic, you know? That that's that's less. That's less of a challenge. So those sorts of things. I think that that monoculture in in, in technology and cybersecurity is is a real issue.  Nice. OK, excellent. | | |
|  |  |
|  |  |
|  |  | P12 |  | Obviously, an apartment attack on Acdn and also you know, I I don't haven't specifically thought about this and because in part just I don't have sources inside this particular well actually I do have a source, maybe I should look more into this but company like square they manage these point of sale systems you know for all sorts of people and there are even point of sale systems out there that appear not to be square point of sale systems but actually rely on square because they they just use square APIs for everything and like you just wouldn't actually be that hard to get inside square and turn it off. You know I can't imagine that they're.  Ready for, you know, a Chinese apartment. It just. And again, maybe they are. OK, maybe they are. You know, maybe maybe cease is in there. Maybe they have former NSA people. But it seems very unlikely to me that that's the case. So yeah, you know, turning these kinds of of payment service providers off like.  I really it seems so easy to do that it seems unlikely that someone at some point won't try it in the next 5 to 10 years. Just be like haha look American capitalism doesn't really work. | | |
|  |  |
|  |  |
|  |  | P12 |  | First of all, so they have a short lived time impact. I think these misconfigurations, but there's scope while they are off can be really big and and I we saw this with Facebook, right, Facebook messed up their BGP configuration and everything. I'm sorry Meta every single meta product was offline. You know Meta's you know like Facebook was offline and Instagram was offline. And I think they even own other other properties that were offline.  And what was so amusing about this to me was that the network that runs their internal systems was also offline, so no one could get there at facebook.com e-mail. And also, you know, they have these systems on their data centres with the badge readers. And those were also networked with the same meta networks. So because of the BGP \*\*\*\* \*\*, they couldn't even badge into the data centre to repair, you know, the thing that was. So what I'm trying to illustrate here is like, although all we've all we've seen are \*\*\*\* \*\*\*.  That were like, just basically misconfigurations, if you know how the network fixed together and you're able to engineer a \*\*\*\* \*\*, you know, like an apt, it can be pretty hard to recover from actually, because if you're saying there's an accidental BGP misconfiguration can make all metapods offer a day, you know, again like a A team of Chinese spies. It was like, has nothing better to do but to figure out how to turn off metapods. You better believe that meta, like all meta products, are going to be offer a while.  You know, like you can really do a lot within the sabotage becomes intentional. And yeah, just these systems are more fragile than we expect. So what would that look like with Cdns with, you know, square? Whatever. Yeah. I mean, these systems could be down for days or weeks even, you know, if they're really, you know, putting intention behind this. | | |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 33 of 316 |  |
|  | | | | | | |
|  |  | P12 |  | Anything that has has to do with CDN failure can mess things up, so you have misconfigurations. I mean this happens. This happens not infrequently, but like Acdn, will this configure something and like all of their customers go down? Of course the problem is even people who are not directly their customers may be rely on a font or a JavaScript library that is hosted by one of their customers. And then that thing goes down and causes this cascading failure. So yeah, misconfiguration of Cdns I mean. | | |
|  |  | P14 |  | And | | |
|  |  | P14 |  | And of course, as we rely on ever more interconnected back to my point about the Internet of Things. | | |
|  |  | P15 |  | AI and computer technology like is the risk that is is worrying in terms of or it's it's an unknown and it's the interconnectivity of the sort of asset management systems and data management systems and all of these things are sewing interconnected that if you have a failure in one and sort of not being able to understand in advance what the ripple effect would be on those systems.  And I think that the more things are automated, the more things rely on on additional technical systems and technical solutions.  Then it's sort of increasingly interwoven with each other and then becomes increasingly difficult to understand.  Where that happens. | | |
|  |  |
|  |  | P16 |  | Yes, yes, yes. Because the tool they have at their disposal has some level of, I wouldn't say consciousness, but has some level of autonomy and automation that will actually that makes it.  Do things at a scale that.  An untrained or unskilled mind cannot comprehend.  So they just see, you know, a machine able to.  Achieve certain things, but without fully comprehending that how it it it's doing that and then they're not understanding the all the all the implications of their request in terms of.  Neutralising or harming the whole you know the the the targets systems. | | |
|  |  |
|  |  | P16 |  | You know the the the, the system replicated and just kind of.  Went a wire and just went all all around the world and paralysed a lot of companies so that that's the idea of propagation. You know you have something in mind that may be a very contained attack. But then because you it's becoming so complicated and so complex. Even for the goodwill attacker, you know it cannot understand all the.  The complexity of the whole ecosystem and might just produce results outcomes that they never kind of actually wanted to to achieve. So that's that's you know this kind of propagation, something that gets out of control.  And not because someone wants to pose major havoc, but just like they didn't think through exactly and they didn't have a clear map of the interconnectedness of our digital ecosystem.  Exactly. Exactly. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 34 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | So that's a little bit what you asked me to to clarify a little bit my propagation kind of analogy, I think that's I'd like to connect it to. I didn't, I'm a slow thinker, so excuse me but but I think that's what what is concerning to me is that this kind of propagation.  Why I think it is important for us to pay attention to it? Is it because it's an emergent effect and because it's an emergent effect?  It it's not something that we can model as easily using kind of classical statistical techniques and all of that because being emergent.  Not easy to predict or to anticipate, because no one exactly understands how it appears. You know it's it's not the accumulation of all the properties of the existing systems being put together just by putting those systems together, we are creating interactions that are.  How to predict to very difficult to model at at at the scale that we are operating that makes it really kind of risky because it it it will surprise us. | | |
|  |  |
|  |  | P19 |  | Now on another.  So the the specific sort of thing then you're thinking about would be an attack on a power state or power station being White, tack in some way, maybe causing knock on effects to another power station causing their hospitals.  You know these, these so called cascading effects like that you might be the worst.  So the the reason work going on on in complex systems and in fact there's a there's a workshop next week in Germany.  There was asked if I wanted to go to it.  In fact, I can't go to it, but I'll turn up at the end of it and we'll talk about.  What was what was presented there?  Yeah, the study of complex systems and including cascading effects is something that is leading to be revisited. | | |
|  |  |
|  |  | P19 |  | So so xxx, getting effects would be a a a real nightmare.  Yes, kind of scenario and you get particularly if you get polo Tages that cross communication failures, communication failures that that could affect future complex power system.  Indeed, yes, yes, which is 1.  One of one of the issues that I think needs to be urgently addressed these these are among the the significant problems for the fujia if, if if terrorists begin to understand how they they, they could cause one of these effects. | | |
|  |  |
|  |  | P21 |  | Yeah, I think that's certainly a risk to underestimate.  Some of those consequences. | | |
|  |  | P21 |  | Yeah, I'm. I'm happy to send you our paper because for ransom, or at least we've come up with a whole taxonomy and we've sort of described first order harm. That's your organisation and the staff 2nd order. That's your patient in the hospital. Your student in the OR someone in your supply chain has a ransomware attack. And then third order. That's for us on a national level. That could be a societal national security economic.  So those are sort of the big order and it's really hard. It's really hard because the farther you move away from the immediate impact.  The harder it is to attribute it to a certain incident, whatever you see and the hard it is to keep a keep it, keep track of what's what impacts you're talking about in the 1st place. And often organisations have very, very little even for ransomware. Organisations have very little understanding of the harm that they're actually experiencing. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 35 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Change Itself Brings Risks** |  | | | | | |
|
|  |  | P15 |  | The sheer fact that it is a change in the way people are going to do things is itself does bring its own risks. | | |
|  |  | P18 |  | The rapid nature of change as well.  Umm. Which you know, all of these can be flipped around to be a positive as well. You know the the rapid nature of change means that.  It becomes difficult to.  Maintain you know, as an engineering maintenance.  A good example of that is.  The cybersecurity you know, updating your cyber arrangements is is a classic example that if you need to prove a piece of software is doing its thing.  That takes a long time to do that, and a lot of testing if then you recognise as a vulnerability with it, and then you make a change to it, then you have to do all that proof again. | | |
|  |  |
|  |  | P4 |  | one of the concerns I've got is around advance if we advance let's say a technology path to quickly such that in automation is taking control without people really understanding the implications of that.  Uh, and you get something bad happening because people don't don't understand what automation was supposed to do.  That that sort of worries me a bit.  And that and that's and that is as you described as a social technical problem, it's not simply an issue with the technology, but the history of all the courses that led to that, that instance to the happening as it were. | | |
|  |  |
|  |  | P6 |  | The visualisation is starting now and did not yet happen. This makes it so difficult if they have now a digitalisation, a very quick one.  Cannot learn how to operate the system, how to protect them and that's so important that this is understood not only for nuclear power plant operators. I | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 36 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Clarifying Risk and Incident Managment Priorities** |  | | | | | |
|
|  |  | P14 |  | one of the key messages from that conference was, but the most important thing UKPLC could do would be to really get its risk of management sorted because, you know, people get fixated on, say, a particular threat.  Without necessarily thinking about what are the harms that that threat is causing and what should we worry about? How much should we worry about so very simple example, judges come from subsequent conversations with National Crime Agency you can imagine.  I'm not saying this is true or not because I don't know if it's true or not, but you can imagine voices inside the National Crime Agency arguing for resource to be deployed to deal with a particular challenge.  And some will be calling for work on illegal migration and some will be calling for work on child sexual exploitation.  Now stand back and just think about the harms. It's very clear the harm from CSE child sexual exploitation is profound not only to individuals, but it affects their education, employability, the knock on effects. It can go through generations so substantial.  Argued. I'm not saying this necessarily, but it could be argued that illegal immigration is quite good in an ageing population if it's bringing large numbers of younger workers in who are eager to work and might end up paying taxes, they could actually be beneficial rather than harmful. So, but you could have two voices, perhaps politically inspired, saying, you know, we've got to do something about the immigration. And of course, we've talked about politics. That might be an important factor to bear in mind in terms of cost. If you create civil disquiet.  And cause all sorts of problems because the the indigenous population is now not happy with all these bloody migrants and blah blah blah. But yeah, so focus there a proper risk management approach which thinks through identifies what the threats are, identifies where the vulnerabilities are, identifies what the, So what questions about what, the consequences, the threat penetrates the target and causes those vulnerabilities.  To to work through. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  | P15 |  | So like what? What are the strategic priorities? What is it that we're even trying to achieve in terms of delivering a service and kind of what what is the minimum service required because effectively you're looking at for CNI, you're saying this is critical to the country to have these goods and not these services and provisions. And therefore it's basically essentially you're thinking about.  The UK as a as a as a business and doing business continuity.  But you need to know what the business's objectives are, what the business is trying to do, and I don't think that that I don't think those things are always clear. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 37 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Class Structure Asset or Not** |  | | | | | |
|
|  |  | P9 |  | Yeah, so, so future, so think this thing about what the future human is. I mean what it means to be a human being for a long period of time is around your social network. And it's about your experiences and what you know when you apply them, if you go back to the old model of the class structure was the working class live off the sweat of their brow, the middle class live off they the quality of their their thoughts and and the upper class live off the value of their assets and we've we had a period from you know the interwar period perhaps through till the late 1970s when that will smoothed out when there was massive redistribution of wealth.  Empowerment, explosion of the middle class because finally, wealth let the working class move up and the aristocracy lost all of that land value and everything. And then we put rent practises back in place in the late 1970s and rent generation now means we've got an asset owning class and everybody else, and the asset owning class like to think that everyone's in the asset owning class, but they're not. And so that's one of the first things is that we've got this massive wealth disparity. That means there's a differentiation occurring. And for people who who are in that happy place, the human experience of fear.  Hunger that completely disappears, and so they're free to think completely differently. And they've been there long enough now that they genuinely they're like, like the audience again. They genuinely think it's the way that the world works and that they deserve it, that so that creates a different social culture. And you can see that in the way they engage with things like Bitcoin and nfts and things like that. They, they, they they own the world and they're not scared of the consequences of that. And for those of us that grew up scared of money and scared of missing a meal, will never ever be able to join that mindset. It's just a completely different thing. So the technology is is moving in, in that sort of direction. I mean, you can see that wandering around in their cyber trucks with their.  Go goggles and things on it. That's fantastic. | | |
|  |  |
|  |  |
|  |  |
|  | | | | | | |
| **CNI** |  | | | | | |
|
|  |  | P20 |  | It's what could terrorist groups cause to fail, which would lead to widespread loss of life and and you know that they were obviously concerned about, you know, terrorist attacks against the financial system, against, in transport infrastructure, against hospitals.  And now all these things have cyber vulnerabilities as well. So yeah, I mean I think it's, I think it's particular.  Discourse that stems from that post 911 environment, the phraseology, the terminology, the lexicon we use.  Really influenced by by that by that particular hapune history. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 38 of 316 |  |
|  | | | | | | |
|  |  | P20 |  | Well, I think is it. Is it Caesar and was it's either Cecil the Department for Homeland Security is the one I've referenced before.  Who define has have a specific.  Definition of what critical is infrastructure looks like. So if you look at critical infrastructure on the Homeland Security website, they talk about networks of highways, bridges and tunnels, railways, utilities, buildings.  Transportation, commerce, clean water, electricity, et cetera, et cetera. But I think actually their definition has widened to include things like again Internet services.  Election systems and a governance infrastructure around elections and various other things. So I generally tend to look at the CISA definitions, or reference to CISA definitions, or the Department for Homeland Security ones. I may be a bit US centric in that regard, but. | | |
|  |  |
|  |  | P20 |  | You know, I I sort of have a feeling that it it's things that if they go horribly wrong might get me not elected. Next time is probably something in the definition.  I I don't know. Yeah. | | |
|  |  | P20 |  | Yeah, I mean critical I think is an important and interesting definitional term. Right. And the way I think about it is what is critical to the effective and safe functioning of society. If you turn something off, what what is going to lead to a societal failure or or loss of life to a significant degree. So it's the things that are critical to keep operating, to enable society to function. I guess that's the way I'd think about it.  I noticed the NCSC have their own kind of web page on C and I and how they think about it and defining it. I imagine it's not dissimilar to to the way the US defining it, and indeed they they cite Jenny Lee, who's director of CISA, in that Web page. So they're obviously leading probably on the way. The Americans have understood it.  I mean, I think it's interesting. I mean, I would contextualise the definition and concept too. I mean, I think a lot of this comes from the post 911 era.  You know the Department for Homeland Security was created after 911 to protect critical national infrastructure in America from the terrorist threat department for whom no Homeland Security is obviously involved in its mandate. Since then, to take on new areas, areas of responsibility, not least cybersecurity. So.  You know, it's. It's what I think historically if we think about this, this discourse of critical national infrastructure infrastructure emerging from that post 911 environment. | | |
|  |  |
|  |  |
|  |  | P20 |  | So I've been interested in following the debate about what we define as critical national infrastructure and and its widening.  Scope and definition I guess so yeah, my my research has has intersected with all those things. | | |
|  |  | P20 |  | The way I've seen it defined again by US authorities is they they sort of define it by sector in within society. So you know, they'll refer to transport, the transport sector, they'll refer to the energy sector, they'll refer to finance. Now, you know, obviously banks and financial systems, I think are part of their definition.  They'll refer to the health sector they're referred to in Internet telecommunications infrastructure. So I think the way the way that I've understood it and the way that.  I think certainly the American Government understand it is they take a sexual approach to what is critical in that national infrastructure. I don't know whether they have a specific definition of of the term critical infrastructure or critical national infrastructure, but it's my understanding that they look at it in sort of a sectoral way and look to define which sectors constitute critical nap national infrastructure because of course then Department for Homeland Security, for example, then has a mandate to protect that. | | |
|  |  |
|  |  | P20 |  | We started off with the definition of. There are 13 different aspects, but there is vague as the ones you're talking about. You know transport and and the the definitions. This is. This is why I was asking you because the definitions seem extremely vague. You know, they say it's transport, but not all transport. So so it it. At the moment I'm kind of getting a feeling it it's it's.  It's critical means whatever I want to include means politically important. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 39 of 316 |  |
|  | | | | | | |
|  |  | P20 |  | Infrastructure so it provides clarity in terms of the functionality of government departments. How are you defining it in your project, Charles? | | |
|  |  | P23 |  | They're they're, in fact is a statutory definition.  I can send it to you if you email me afterwards, I could send it to you.  There's also policymakers have proposed some, but the president gets to in the US, the President gets to establish an area is a critical infrastructure.  So the definition can say X, but then the president can say I hereby declare so and so critical infrastructure. | | |
|  |  | P23 |  | We | | |
|  | | | | | | |
| **CNI Attacks No Longer War** |  | | | | | |
|
|  |  | P12 |  | that I think that the kind of the end of the Pax Americana and a return to more ad hoc and sustainable conflict is really the biggest change that I'm tracking. I think that we've been playing security on easy mode because.  Disrupting critical infrastructure.  Would have been out of bounds up until very, very recently and for a variety of reasons and sort of, I would say beta tested by ransomware crews who do this for profit and operate with impunity, you know, within Russia typically or North Korea, you know, we've seen that actually there won't be probably a military response even to critical infrastructure.  You know, attacks, at least so far, and I think that that.  New reality is created. What I believe to be the most dangerous kind of change recently. | | |
|  |  |
|  |  | P23 |  | then we have all the things below that that are gonna be a continuing problem of the so-called Gray area.  Attacks on critical infrastructure that are less than an act of war yet are profoundly annoying.  Expensive undermining of government trust. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 40 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **CNI sectors dependent on Telecoms and Electricity** |  | | | | | |
|
|  |  | P10 |  | I think you know that of telecoms.  I know that's part of the the critical infrastructure, but thinking about just loss of those kind of basic services kind of water for cooling service, you know loss of loss of of power | | |
|  |  | P10 |  | It's it's and I think this is legitimate as as a concern here, we're losing. We're losing resilience. So I sort of so I think re retail becomes critical. If it's eroded, the kind of the physical, let's say, retail infrastructure to the extent that there's nothing to to pick it up.  And that and that's true of, you know, you could think about kind of food supply, it's about us almost a supply chain question, isn't it? And various other modes just as we always find with something you know interferes with that kind of system. | | |
|  |  |
|  |  | P14 |  | Sewage systems fail.  Transport systems collapse, health systems collapse. That's major. OK, so a major solar storm. | | |
|  |  | P14 |  | Because supply chains go down, communications goes down.  Government can't communicate with the people to provide any level of assurance or reassurance.  Water supply runs out. | | |
|  |  | P14 |  | . But that was I just remember.  Thinking that was an extraordinary list of everything, as people were just sort of reflecting on what the hell goes wrong. The answer was some very serious stuff. Yeah, yeah, I've given a sense of it. Transport telling. It's the telecommunications because often radio TV, because all these sorts of signals have been that badly damaged. GPS goes out. | | |
|  |  | P15 |  | a lot of those risks would look similar.  To a national power outage or a regional power outage, which there's been an awful lot of thinking and mostly the thinking is that would be fairly, fairly catastrophic, but it would be so catastrophic that literally everything else would have failed at the same time. So trains wouldn't be your last issue. And there's a there's.  I think the the biggest risks are the ones where.  Things are so uncertain about where they might happen or how it would trickle out, or we didn't. We haven't done the thinking around those things | | |
|  |  |
|  |  | P19 |  | So the the specific sort of thing then you're thinking about would be an attack on a power state or power station being White, tack in some way, maybe causing knock on effects to another power station causing their hospitals.  You know these, these so called cascading effects like that you might be the worst. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 41 of 316 |  |
|  | | | | | | |
|  |  | P19 |  | So so Chris, getting effects would be a a a real nightmare.  Yes, kind of scenario and you get particularly if you get polo Tages that cross communication failures, communication failures that that could affect future complex power system.  Indeed, yes, yes, which is 1.  One of one of the issues that I think needs to be urgently addressed these these are among the the significant problems for the fujia if, if if terrorists begin to understand how they they, they could cause one of these effects. | | |
|  |  |
|  |  | P22 |  | Yeah. So we are so dependent on electricity.  And telecoms is dependent on electricity. | | |
|  |  | P22 |  | More people are dependent on electricity as part of infrastructure.  And the technology. | | |
|  |  | P22 |  | National Preparedness Commission and xxxx, who's to share that.  As as his nightmare that if electricity, electricity in some areas of the UK went out for three days.  The food stocks of the UK would be shot because of lack of refrigeration.  And you see there would be food riot. | | |
|  |  | P24 |  | Many things, many other assets and components cannot operate and then.  I don't know your.  Food in the fridge is perished because if this calculate failure is not.  Addressed in a timely manner. Then many things can escalate so.  And I believe part of it is related to.  Risks and hazards to computer elements or software elements in critical infrastructure. | | |
|  |  |
|  |  | P24 |  | if there is software failure in the energy system, which I I believe it's like the main, it's like the foundation of.  Society somehow? | | |
|  |  | P5 |  | for me the biggest one that's more immediate is the remote communications because when you have multiple SMR's in a geographic area, they're talking about having maybe one control room that feeds to all of these reactors.  And so how do we secure those communication lines?  You know whether it's hardwired or wireless or whatever it might be.  And you know, it's not just monitoring, but they're looking at control through these remote communications.  And so that's gonna be a really big deal to verify that we can convince people that we have a cyber secure communications network there. | | |
|  |  |
|  |  | P7 |  | A very key critical national infrastructure sector as well, right? | | |
|  |  | P7 |  | national infrastructure and we talk about now energy and and and defence, but telecoms is is a very. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 42 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Complexity Increases Risks** |  | | | | | |
|
|  |  | P19 |  | And then to have redundant systems and and OS so that that's that's been addressed and being addressed.  But lots, yes, yes | | |
|  |  | P19 |  | I mean they, they mean that there's even more data.  Course, yeah, even more data that's been stored.  And and the more data that's stored, the more the haps important is to protect it. | | |
|  |  | P19 |  | Thanks to the Internet, yes, operational technology is good discussed including the yeah, any kind of automated.  But yes, transport systems, yes.  Ohh, any of these is likely to be compromised if if if attackers have a will to do it.  And that is an increasing trend, doesn't it?  There's unfortunately it doesn't.  Yes, yes, yes.  And that the more the more computing, frankly that goes into the systems.  The more vulnerabilities potentially get introduced, yes, yes. | | |
|  |  |
|  | | | | | | |
| **complexity lead accidents** |  | | | | | |
|
|  |  | P10 |  | That Tropic cascade we've already been talking about, yeah, absolutely, absolutely. And yeah, the interconnectedness around supply chains, but, but particularly the the sort of the sort of cyber connection here is is, is, is critical, absolutely.  The other thing that might be worth mentioning is this is sort of got a natural world agricultural metaphor to it as well. So I'm just sort of doing GCSE sort of history and looking at, you know, the American Dust Bowl and and the problems with monocultures.  We the the the risk of monoculture in security subsecurity in particular is if everyone, let's say, everything government is run on Microsoft because they're very good and you know, I've no criticism of Microsoft. But if it's a monoculture, you get one floor. Great, you've got one floor and it gets, you know, it kind of goes across the piece and there's again just looking at good data. Microsoft, if you if I am a malicious person and I want to you know create a but I'm I'm going to target Microsoft because it is.  It it is buggy and it's going to have, I'm going to get my greatest bang for my buck. I'm not going to be trying to work on something. What is it that submarines run on? You know something that's really archaic, you know? That that's that's less. That's less of a challenge. So those sorts of things. I think that that monoculture in in, in technology and cybersecurity is is a real issue.  Nice. OK, excellent. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 43 of 316 |  |
|  | | | | | | |
|  |  | P12 |  | That's a really interesting question. I don't know about enough about the electricity grid, but my take on this and maybe this is just from California, is that we have a monopoly. You know, there's just this monopoly on, on and and they're not very good. They should probably be naturalised, but but there there's only one, so they only need to coordinate with themselves and with the other providers who you know, border like the region.  With cloud flare, I think it's a little bit different because they provide overlapping services to the same customers and so the chances that they do rely all on the same data centres all throughout, you know the world that seems to be much higher than the idea that like.  PG&E and, you know Pacific Edison both rely on the same and that seems less likely to me.  But maybe I'm wrong. Who knows. I could definitely be wrong about that. I really don't know enough about how the grid works and same with water like. I just don't know. | | |
|  |  |
|  |  |
|  |  | P12 |  | You're relying to have done due diligence in a way that you know sends sacrifices, some trade secrecy or competitive advantage. So what you would what you would need them to do is go to, you know, if your cloud player employee go to Google and say, hey, Google, we have some deployments here. Do you have some deployments here and another each needing to sacrifice some trade secrets to one another in a way that really us could even be seen as anti competitive? If you have, you know.  The wrong interlocutor, who learns about that conversation. So I think that's really dangerous. Like the kinds of things that we would need for them to be doing. It seems really unlikely that they would be able to do practically at least at scale without being forced basically by in some kind of, you know, safe harbour, you know. | | |
|  |  |
|  |  | P12 |  | It's really hard for me to evaluate that claim because it does feel that we've already reached a level of network size that would be pretty difficult for a human to reason about.  So I think we're past that Inflexion point. So then would there be some other Inflexion point where like even I OK, here's the way I would think about this question, right?  With these interconnection points I or with you know, this kind of general problem, that's like kind of graph complexity, right?  You rely on automated solutions to identify issues. I imagine that those systems have some kind of computational complexity, so you have to do some graph search. Is that how does that graph sort? Scale? You know, is it in NP? You know, I actually don't know about how these systems work in practise, but I think what you would want to do if you were trying to evaluate those questions like OK of these systems that are actually used to evaluate interconnection.  Are there any problems that are in NP, and if so?  When or how would we expect that to become a problem? Like at what point would we expect this to be impractical to actually compute? And then how are we going to deal with that if there's no good answer, then I would say yeah, maybe. But otherwise I would kind of my instinct on this, honestly, is like we're already there, like we've been there for maybe five years already.  And also you know this maybe not answering your question, but I'm much less concerned with the complexity or of interconnections and that I am with the opacity of interconnections. | | |
|  |  |
|  |  |
|  |  |
|  |  | P12 |  | Yes, interesting.  And that's probably repeated in many situations. That's a kind of that's, you know, and A and a cross critical infrastructures. You know, you might find the electricity again they won't be coordinating on what could go wrong. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 44 of 316 |  |
|  | | | | | | |
|  |  | P12 |  | So it doesn't bother me that Cloudflare's network is very, very complex. What bothers me is that I have no \*\*\*\*\*\*\* idea how it works, because that means that I can't understand. Yes, like they have a private. So what? I request the New York Times, right. I don't go to New York Times server. I go to my ISP. It's in downtown Oakland and downtown Oakland. You know, some box just delivers. The New York Times to me. And I have no idea what happens on the other side of that. And from the New York Times perspective too, they handed to Cloudflare and they have no idea what happens on the what happens in between me and the New York Times is a mystery to everyone but Cloudflare.  We don't know what is inside there and look, if you don't believe me, go do a trace route on Google your it'll go. You'll see. It goes to your ISP and then it disappears into Google's network. And then it just comes right back out with some I don't have no idea what's going on. You know, this isn't a we don't know how this works. I'm sure Google does. I hope. And to an extent, I'm sure that they do. But I know that Cloudflare doesn't know how Google's network works, and Google doesn't know how Cloudflare's network that is much more concerning to me than the complexity. It's the opacity to the parties that matter.  Possible to do risk management for any one of these critical infrastructure firms? That's very scary to me.  Like, are there correlated dependencies? Are there correlated failures because it could be that they all rely on this one data centre in downtown Oakland and you know a PG E outage breaks like everything for the whole East Bay.  That would be really stupid, but I do think that that's that. I think it's more likely than people expect, yeah. | | |
|  |  |
|  |  |
|  |  |
|  |  | P13 |  | Yeah, I'm sure that's true.  I mean, I I'm just looking at the the history of systems and systems of our, particularly in the software domain. The more complicated you make something, the more likely it is that you haven't tested everything that could happen.  Therefore, the the chances of errors goes up. | | |
|  |  | P14 |  | As more systems become connected.  There is greater complexity. | | |
|  |  | P14 |  | And | | |
|  |  | P14 |  | And to try and encourage that sort of system of thinking.  So yeah, it's got as the world gets more complex and more connected, that's definitely a danger. | | |
|  |  | P14 |  | A potentially major issue came forward. It's an issue now.  I mean the the famous one is from is it the early 1990s when the the lorry drivers who delivered fuel went on strike? | | |
|  |  | P14 |  | Part of the critical astral infrastructure.  But and you know, they wanted to deliver a message, but they had never imagined that babies would be dying in hospitals because. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 45 of 316 |  |
|  | | | | | | |
|  |  | P14 |  | Fuel wasn't getting through to hospitals, generators there or or wasn't getting to the generators. Generators fell over, incubators fell over. Babies die. Don't have that actually happened, but it was getting quite close to that happening. And I think they abandoned the strike at one point when they suddenly realised the repercussions of what they thought would be quite a simple and relatively symbolic. | | |
|  |  | P14 |  | And yeah, that's one small example of it.  And I think.  I think that might have led to the creation of the civil contingency secretariat being set up. | | |
|  |  | P14 |  | And | | |
|  |  | P16 |  | It's the the political scientists they call that a trans boundary crisis, because usually, you know the the people like us, you and I, studying crisis. We're usually studying a specialised in this in a in a in a discrete area of human activity. So I'm a criminologist. I'm interested in in fraud. People are working in different sectors. But now because of this interconnectivity, different sectors are.  Connected to each other and they operate under different assumptions and they have different cultures and they have different.  Frameworks in place and when the crisis crosses a boundary, then it transforms and it is being made sense of using different tools and it's becoming difficult for people from different areas to communicate with each other because their mental models are different. So that's so that's, you know, those are the different variables that explain why this is.  Introducing.  Complexity of risk, that is that are not that is not as easy to handle. Then the more conventional crisis contained documented, more predictable, easier to respond to, and and so on and so forth.  Yes, yes, yes. | | |
|  |  |
|  |  |
|  |  | P16 |  | So that's a little bit what you asked me to to clarify a little bit my propagation kind of analogy, I think that's I'd like to connect it to. I didn't, I'm a slow thinker, so excuse me but but I think that's what what is concerning to me is that this kind of propagation.  Why I think it is important for us to pay attention to it? Is it because it's an emergent effect and because it's an emergent effect?  It it's not something that we can model as easily using kind of classical statistical techniques and all of that because being emergent.  Not easy to predict or to anticipate, because no one exactly understands how it appears. You know it's it's not the accumulation of all the properties of the existing systems being put together just by putting those systems together, we are creating interactions that are.  How to predict to very difficult to model at at at the scale that we are operating that makes it really kind of risky because it it it will surprise us. | | |
|  |  |
|  |  | P16 |  | I think that's so that's I think goes back to you asked me my concern. I think that's for me that's that's it the you know the complexity, the emergent effects that.  Are being generated by that complexity that we are not.  Modelling and that we are not.  Probably properly understanding. | | |
|  |  | P21 |  | Small steps over a long period of time with very little systematic effort or budget or knowledge, really like I don't want to blame the school for that, but that's just how things developed as well in universities.  In those instances, I could see how that that can be become a problem, yeah. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 46 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | Yeah, I I think it depends on how interconnectivity is is achieved.  If we just randomly plug in more things without understanding where failure points are or where where more measures are needed for example, then I think yes. But.  Per say, connectivity isn't isn't a bad thing.  Yeah, I think it's more. | | |
|  |  | P21 |  | It goes a little bit back to the workshop discussions now. It's still we that can come up there. I thought I wasn't quite convinced by that. I think in some ways that sort of easy to think that interconnectivity is necessarily a bad thing. But I think it can also mean that some things are more secure or you're sort of if you become part of the sub network, you might for example have to meet there already higher requirements. If you think that you are now acni provider then.  Maybe that means you have to.  If she and I provided might be more sad and mature, and their hygiene and then you might have to meet those the same requirements. So I don't necessarily think that that's the case, but I think in some instances, for example, schools where more interconnectivity has been done instead of. | | |
|  |  |
|  |  | P23 |  | You know, there's this amazing book by Perot called normal accidents.  It's just fantastic contribution that would suggest that as complexity increases, there's gonna be so called normal accidents and and then you have this other group of people, the high reliability organization, people who say no, actually, there's all these things that that work like like Airline flying is an example of highly complex thing and it's actually really rare to die for there to be a crash.  So there's a debate between these two and it where have come out on this is I'm the high reliability organizations, they require big bureaucracies and and so people say AI is gonna kill all the jobs I'm making to wonder if AI is going to require the ultimate kind of management bureaucracy. | | |
|  |  |
|  |  | P23 |  | Where we're constantly kind of checking things and and so on.  So that's like I don't.  So there are so complexity increases, there's normal accidents, motor vehicle, sure.  But then how do you explain things like airlines and and actually nuclear reactors, which rarely in fact, meltdown and and so on? | | |
|  |  | P23 |  | So I don't know the answer to this stuff, but I wonder if it's.  If we're gonna have a, we're essentially gonna have to have an AI bureaucracy to deal with the things that are going to happen. | | |
|  |  | P24 |  | As a as a society, not being able to recognise the boundary like OK, this was until this point it was because the software was not working properly, but it also opened the window for cyberattacks. | | |
|  |  | P24 |  | Hmm, I I haven't thought of that before. I I somehow had this idea that that this. Yeah, I know. But no, no, my.  My opinion that would say that would would be that.  Yes, I agree that systems are a quite interdependent and interconnected. But somehow I thought that it could be easier to distinguish the cause of failure.  But now that you posed the question, yes there is. There is a high chance for them to be like mixed. | | |
|  |  |
|  |  | P4 |  | So these are people that work in switching rooms, signaling where things go. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 47 of 316 |  |
|  | | | | | | |
|  |  | P4 |  | I remember at the time telling people I'd say, what do you think the most critical issue that people face and they talk about denial of service as a malware?  No one thought about illegal migrants? | | |
|  |  | P4 |  | So if you're gonna carriage that goes over a bridge, and that thing is too heavy, then the bridge, the bridge could sort of collapse. | | |
|  |  | P4 |  | One of the worries they had was that people were trying to sneak onto rails and that was changing.  The sort of weight and stuff.  And there was some people that would deliberately doing it to try and make money.  But The thing is, a lot a lot of the infrastructure is very tied into the weight of of carriages. | | |
|  |  | P4 |  | And one of the concerns that she she highlighted that is, of course a concern is the idea of a bad actor.  Uh feeding misinformation in into the system to call something undesirable, to to, to basically happen. | | |
|  |  | P4 |  | collaborative work on critical infrastructure on the Greek Railway and one of the and at the time one of the big worries they had was actually was actually migrancy.  Because what was happening is people were starting to sort of cross into sort of Lesvos, get into Greece and trying to get into other parts of Europe. | | |
|  |  | P4 |  | I'm not on the on on the right and structure, so something that looks like an accident but isn't really an accident and and that was so the the the paper talks about about that as an example and that's real, I mean that's that's that's critical infrastructure for you. | | |
|  |  | P5 |  | OK, that's one of the things that we talk about in cyber informed engineering is complexity versus simplicity.  And one of the recommendations is to make it as simple as possible to perform only the function that you need it to perform of the system.  So for instance, you buy a programmable logic controller.  It may have two or 300 functions that it's capable of.  You basically configure the five functions that you want it to do for your process, and then all of those other hundreds are there.  If an adversary gets into that PLC, they potentially can enable those and do things that it wasn't designed for.  So our push is, if at all possible, remove all those other hundred functions out of that PLC, if that is possible.  The bottom line is you only want the system to perform the functions it's supposed to. | | |
|  |  |
|  |  |
|  |  | P7 |  | It's inevitable that systems become more complex.  But then when they do it's it's harder to it's harder to contain. It's harder to understand. It's it's harder to debug when when things when things go wrong.  When when it comes, when it comes to people being able to distinguish what is malicious versus what, what is an accident?  The obvious answer is yes, but I'm not sure this is the sort of more, more critical point, so long as you know if the consequence is the same.  You need to revert the consequence, right? That's the sort of first first thing that you need to do.  Whether it comes from a from a deliberate action or or from an accident might be a sort of second level analysis. It might not but but but. But it also might, but complexity is is more general. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 48 of 316 |  |
|  | | | | | | |
|  |  | P7 |  | Shall shall I carry on the this, this the second thing is coming back to the to the AI is the is a sort of intelligence that we need to embed in those in those systems.  And and you know the.  I mean, it's still early days, but you know if you want to the to the complexity mix, the fact that a you might have to do learning over resource constrained environments, B you have to integrate data from diverse sources that looks different, blah blah blah they cannot, it cannot readily be integrated into a coherent model it it makes this an even more complex complicated space.  And they say, and I think last but not least, the the third is OK, let's assume we solve this all these problems from a technology point of view, right?  How are we gonna? How are we gonna get the companies and and then the critical infrastructure providers to run any of these on their on their systems, what do we need to do?  We obviously need to get it somehow certified. We need to get it regulated. We need to get the operators to understand an interface with it, which is one of the questions you alluded to.  Elsewhere. So this kind of I think ecosystem organisational integration, I think it's it's it's also very important and it's at the end of the day, I think it's the, it's what it will make the difference from having nice scientific papers about something versus having something deployed in on on real systems. | | |
|  |  |
|  |  |
|  |  | P7 |  | More generally, a problem and and then it's something.  Critical infrastructure sectors are are that that's part of the reason why they are averse to to modernization, because they see this increase in complexity coming. And I think it's fair, it's a it's a fairpoint.  So again, lots, lots of work for us to make sure that you know we we we we keep you know we keep having a a a sustainable economy society which.  More and more depends on technology. Technology is getting more.  More complex.  But how this then is embedded in a in in a culture that's you know it's stays trustworthy and safe. It's it's a very big challenge and that's good because we like big challenges because otherwise we'll be out, we'll be out of job, right. | | |
|  |  |
|  |  | P9 |  | That's, that's where you end up.  So you know, I'm slightly sure, but within the Christian life, Christian life, infrastructure space, what we're seeing now is we're going to move from methane gas pumping through networks. Those asset base is about Â£14 billion worth of underground asset there. That's going to get completely useless. So there's going to be a lot of work put into trying to reuse it or something. Is it what you just put hydrogen down there, OK, hydrogen network, you can't pack for pressure carries per mass. It carries 1/3 less the amount of energy it flows that very, very much faster and it leads a lot more easily. So you could upgrade your system, the maintenance schedules are higher.  And you've to reconfigure the feed in and feed out of the system and run and run it to storage, because you can no longer use the network for storage, you're going to have to do that every 30 minutes instead of every 24 hours. Now the complexity of managing that system and then interfacing it with the different contracts because people only want to pay for the kind of gas that they want put into it, that complexity. Now you add electricity, which we've simplified the market enormously by just doing marginal pricing rather than pricing by type, which is going to be coming.  That combined with water.  We're doing hydrogen. The hydrogen economy predicted for the UK will mean we need about three times as much clean water as we currently have in the entire country, so the whole water network is going to get boosted 3% of our energy bill already goes on running water system in the UK, so you can expect that to go up and then you've got the waste, both in terms of waste energy and in terms of the waste products of that, which will then run through a series of efferent networks out for sequestration through the carbon being pumped, that the homeostasis of the pumping lifeblood.  Of a of a of a of a geographic region is going to get much more complex in order to keep it within the bounds of what we can put within the energy envelope of the planet.  I think that's going to be a really interesting problem and I think that is going to happen within the next 10 to 15 years.  15 years we've got no chance of making our temperature targets, yeah. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 49 of 316 |  |
|  | | | | | | |
|  |  | P9 |  | That's | | |
|  |  | P9 |  | The last thing I'll just say on systemic fragility and it comes back to stuff of beer again, is the way you manage a complex system is edack error detection and correction. So you have to assume that your system will fail and you have to put a system in place that monitors it and keeps it within bound. Then you have to assume that that system fails and so on and so forth. And it's how complex organisms like ours develop homeostasis. The digital domain is sufficiently complex that we need to start to think about those correction mechanisms.  We haven't got them all right yet.  So you know that that.  You know when when we see a deviance from what we'd like something to be, we have to think. Oh, what sort of institutional mechanism would have fixed that? It might be digital, it might not. But we should fix every every example with a how can I fix this systemically, rather than sticking plasters? You don't run around picking sticking plasters on you. Try and steer the thing, right? So that's just one. One thought that the relays to all of these.  The other two I mentioned there was the.  Yeah. What would?  Brain the brain thing.  Sorts of qualia injection piece. | | |
|  |  |
|  |  |
|  |  | P9 |  | Intangible. We can't hold it or ship it or move it by the pound, and non exclusionary means I can't actually stop you knowing something, OK? | | |
|  |  | P9 |  | Is around the information flows that flow through this and here my my beef and I'm going to take the opportunity to put it on record again because I always do is we need to start to think in policy terms not about data and information as two separate things.  OK. And I'm gonna. I'm gonna. Semiotics. I've just separated 2 labels. Let me explain what the things are. Data is the physical records of events happening. Information is the anti entropy of that event having happened.  So if you like Shannon entropy, Shannon entropy is information. Data is the physical carrier that's carrying it, and data travels both in space and in time. So if I write a record to myself, that's a data object travelling in time, it's lossy because I can't read my own handwriting, but it's there.  But the information is what I've actually written and a lot of people when because digital makes data look like information because it's so easy to move around. They tend to assume they're the same thing. They're not. Information is non rivalless, non exclusionary.  Economic terms non rival risk means if I if you have it, that doesn't stop me enjoying the use of it as well. | | |
|  |  |
|  |  |
|  |  | P9 |  | No, I was just. I was just looking down the the list in in terms of technologies you mentioned and we've talked general infrastructural complexity, we've talked about the information domain as a piece of national infrastructure and what that might look and feel like.  And we talked about systemic fragility.  And the fact that we may have mechanisms to engage that. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 50 of 316 |  |
|  | | | | | | |
|  |  | P9 |  | Yeah, yeah, it can be exclusionary 'cause. I can keep you from accessing it. I can try.  And it costs money to generate it and maintain it. So it's an economic data is an economic good.  Information is this other thing because they've become entangled.  We are not managing information risks properly. We're managing information risk by trying to manage data, wrong thing to do.  And until we get that right, we're going to continue to have policies that make life harder and more difficult, and that will have implications for privacy that will have implications, implications for risk, ownership. It'll have implications for liability. So we really need to start to grow up and have a conversation conversation that says if you need to know something and I need to know something, we're talking information. Am I. Am I going to facilitate that exchange through giving you access to data?  And that's those are then two separate lines of activity. | | |
|  |  |
|  |  | P9 |  | so I wonder, I wonder what we've got at the moment and they didn't. And they do tend to drift as well. That's one of the other things about really complex systems is they tend to drift into positions. And unless you've got a meta system which is forcing them back in again, they will drift into places you don't. So Stafford beer talks about this in his organisational cybernetics, work around control systems and control systems and control systems. The final control system in societal terms, is a revolution.  And if you if your government system deviates too far. | | |
|  |  |
|  | | | | | | |
| **Critical Becomes Diluted** |  | | | | | |
|
|  |  | P20 |  | mean I think the challenge it provides is from a policy point of view, if you keep adding to what you conceive of as critical national infrastructure.  And you're giving then agencies the responsibility to manage that infrastructure and protect it and secure it. It becomes an ever expanding thing that they're responsible for. And we don't have the resources, the manpower or the regulatory policy or the laws to actually effectively do that. So if we're adding everything into the critical infrastructure bucket and calling everything critical infrastructure and then expecting people to deal with that in effective ways doesn't seem to me very achievable.  From a policy or resource point of view.  There's also concerns that I've heard about you dilute then what really is critical. So if you count everything, then the the term critical infrastructure protection becomes meaningless. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 51 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Cryptographic Solutions to Fake Information** |  | | | | | |
|
|  |  | P12 |  | My question is where are the companies on this, you know, producing kind of cryptographic schemes to, you know, and. And I do think we'll probably just someday see an apple.  Saying hey, we we we allow this now with your iCloud iCloud is the only fully verified authenticated way. So you have to get an iPhone and actually you can't even check the signature unless you have an Apple device. If you have something like but whatever you know honestly that is better than the world we live in today. So I would I would I would salute that and say OK you know deep fix kind of partially solved there and apple and trenches there they're monopoly even more but yeah that's kind of how I think about that stuff. | | |
|  |  |
|  |  | P12 |  | It does seem to me like we as a security community for a long time have had cryptographic tools for dealing with this kind of situation in the form of, like cryptographic signatures and stuff. And I do feel that there were, I mean, there are voices on many sides because the EFF is always kind of these days, in my personal opinion, kind of being really useless or counterproductive. But.  There have been, you know, a lot of civil society organisations that were like, hey, you know, you should consider having some kind of cryptographic scheme, you know, in your national identity card, to allow people to sign content. And I also think that it's within, you know, Apple's power to have some. Yeah, I think even maybe because they use pass keys now. So maybe web authent even allows you some kind of signing key. But to allow, you know, your device to sign.  Contents so that you can say, well, I I you know.  Like there's some evidence that I captured this or whatever, and when the absence of that signature that I can, whatever, you know, those solutions do exist. | | |
|  |  |
|  |  |
|  |  | P12 |  | But maybe I over estimate people's.  So, you know, belief in how these things work because again, this is all predicated on people actually believing the cryptography works. And you know, you don't even think vaccines work. I don't think you can probably be expected to believe the cryptography works. It's even more abstract. So, you know, I don't know. | | |
|  |  | P23 |  | Maybe it's been cropped, you know, but you can say for sure that it hasn't been perturbed for its content. | | |
|  |  | P23 |  | I have a colleague who is working on the kind of end to end. I'm.  A watermark for cameras and other media.  So you can you know when you get the New York Times and there's a photo in it, you will be able to say that photo has been edited. | | |
|  |  | P23 |  | I think the day is not far away where we're gonna need, you know, politicians and other important people to use technologies in their communications to prove that it is that it has integrity. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 52 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Current Situation Poor** |  | | | | | |
|
|  |  | P11 |  | Interestingly, you've positioned this as starting with wherever we are and looking forward, what about the fact that we're in a pretty dreadful position already and none of that's going to actually magically get better in the next so many years given the longevity of assets. | | |
|  |  | P12 |  | it does feel that we've already reached a level of network size that would be pretty difficult for a human to reason about.  So I think we're past that Inflexion point. | | |
|  | | | | | | |
| **Danger from Increased and Opaque Connectivity** |  | | | | | |
|
|  |  | P12 |  | So it doesn't bother me that Cloudflare's network is very, very complex. What bothers me is that I have no \*\*\*\*\*\*\* idea how it works, because that means that I can't understand. Yes, like they have a private. So what? I request the New York Times, right. I don't go to New York Times server. I go to my ISP. It's in downtown Oakland and downtown Oakland. You know, some box just delivers. The New York Times to me. And I have no idea what happens on the other side of that. And from the New York Times perspective too, they handed to Cloudflare and they have no idea what happens on the what happens in between me and the New York Times is a mystery to everyone but Cloudflare.  We don't know what is inside there and look, if you don't believe me, go do a trace route on Google your it'll go. You'll see. It goes to your ISP and then it disappears into Google's network. And then it just comes right back out with some I don't have no idea what's going on. You know, this isn't a we don't know how this works. I'm sure Google does. I hope. And to an extent, I'm sure that they do. But I know that Cloudflare doesn't know how Google's network works, and Google doesn't know how Cloudflare's network that is much more concerning to me than the complexity. It's the opacity to the parties that matter.  Possible to do risk management for any one of these critical infrastructure firms? That's very scary to me.  Like, are there correlated dependencies? Are there correlated failures because it could be that they all rely on this one data centre in downtown Oakland and you know a PG E outage breaks like everything for the whole East Bay.  That would be really stupid, but I do think that that's that. I think it's more likely than people expect, yeah. | | |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 53 of 316 |  |
|  | | | | | | |
|  |  | P14 |  | And to try and encourage that sort of system of thinking.  So yeah, it's got as the world gets more complex and more connected, that's definitely a danger. | | |
|  |  | P14 |  | the Internet of Things is another major game changer, because when the whole world is connected up.  And when you could actually, you know, a sort of some some spotty youth in a basement in Melbourne just wanting to have fun, not necessarily trying to destroy an enemy, but just wanting to, you know, have a little bit of a laugh.  Can connect through and get into some Internet of Things link which then breaks into a bit of the critical national infrastructure. | | |
|  |  |
|  |  | P14 |  | with Ji and ML does offer combined with an Internet of Things which allows everything to be joined up in a. | | |
|  |  | P15 |  | Yeah, you can never test this. You can never test anything. | | |
|  |  | P15 |  | AI and computer technology like is the risk that is is worrying in terms of or it's it's an unknown and it's the interconnectivity of the sort of asset management systems and data management systems and all of these things are sewing interconnected that if you have a failure in one and sort of not being able to understand in advance what the ripple effect would be on those systems.  And I think that the more things are automated, the more things rely on on additional technical systems and technical solutions.  Then it's sort of increasingly interwoven with each other and then becomes increasingly difficult to understand.  Where that happens. | | |
|  |  |
|  |  | P16 |  | Yes. And the and the fact that because we are interconnected but still distant. So if we're interconnected through two or three degrees of separation.  Your future is of no concern to me because I'm not gonna be the one who's gonna pay the price of my decisions being propagated to you and crushing your system. I'm gonna say too bad, so sad. But you know, my incentives are zero, so I'm gonna keep on doing what I'm doing because it.  Serves me even if it weakens you. So those kind of emergent effects when you have negative externalities that I'm pushing to you and you may not have the label of sophistication to understand or to absorb that I'm saying, but that's not my problem. You know my decisions, my systems are perfectly safe because of my decisions, maybe it generates discomfort for you, but fix it on your on your end, you know.  It it may, it may work from my perspective, but from a system level perspective, it's kind of disastrous because it it it generates.  A system where.  No one is looking after the negative consequences of their own decisions | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 54 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | So that's a little bit what you asked me to to clarify a little bit my propagation kind of analogy, I think that's I'd like to connect it to. I didn't, I'm a slow thinker, so excuse me but but I think that's what what is concerning to me is that this kind of propagation.  Why I think it is important for us to pay attention to it? Is it because it's an emergent effect and because it's an emergent effect?  It it's not something that we can model as easily using kind of classical statistical techniques and all of that because being emergent.  Not easy to predict or to anticipate, because no one exactly understands how it appears. You know it's it's not the accumulation of all the properties of the existing systems being put together just by putting those systems together, we are creating interactions that are.  How to predict to very difficult to model at at at the scale that we are operating that makes it really kind of risky because it it it will surprise us. | | |
|  |  |
|  |  | P16 |  | now because of this interconnectivity, different sectors are.  Connected to each other and they operate under different assumptions and they have different cultures and they have different.  Frameworks in place and when the crisis crosses a boundary, then it transforms and it is being made sense of using different tools and it's becoming difficult for people from different areas to communicate with each other because their mental models are different. So that's so that's, you know, those are the different variables that explain why this is.  Introducing.  Complexity of risk, that is that are not that is not as easy to handle. | | |
|  |  |
|  |  | P16 |  | I think that's for me that's that's it the you know the complexity, the emergent effects that.  Are being generated by that complexity that we are not.  Modelling and that we are not.  Probably properly understanding. | | |
|  |  | P16 |  | reasons possibly the one is the complexity of the whole system that no one can can truly understand | | |
|  |  | P16 |  | What concerns me is that.  The the the the label of interconnectivity that we are implementing with all systems being connected to all other systems using underlying technology that bricks that we kind of.  Place here and there without often.  Fully understanding all the interdependency that we are creating.  Might very well.  Create a system where risk is being amplified without us being able to understand how it propagates within the system and leading to you know, a common event that could trigger a general collapse of systems.  So this lack of mission, lack of understanding of the interconnectivity and interdependencies, | | |
|  |  |
|  |  | P16 |  | You know the the the, the system replicated and just kind of.  Went a wire and just went all all around the world and paralysed a lot of companies so that that's the idea of propagation. You know you have something in mind that may be a very contained attack. But then because you it's becoming so complicated and so complex. Even for the goodwill attacker, you know it cannot understand all the.  The complexity of the whole ecosystem and might just produce results outcomes that they never kind of actually wanted to to achieve. So that's that's you know this kind of propagation, something that gets out of control.  And not because someone wants to pose major havoc, but just like they didn't think through exactly and they didn't have a clear map of the interconnectedness of our digital ecosystem. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 55 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | what sorts of emergent effects might there be? Are we talking instabilities or are we talking?  You know, just just sort of something I could throw in would crash.  Unexpected unexpected valid. One thing what I think is valid might crash your system or vice versa. | | |
|  |  | P18 |  | I don't know Internet of Things, that interconnectedness of the digital arena means that it's becomes easier for faults for Miss.  Miss operation of your faults within the system to propagate across multiple systems and you get multiple system failure as a consequence of that. So it's the interconnectedness that comes with digital as well, which also causes causes a risk. | | |
|  |  | P23 |  | You know, there's this amazing book by Perot called normal accidents.  It's just fantastic contribution that would suggest that as complexity increases, there's gonna be so called normal accidents | | |
|  |  | P24 |  | if there's an issue in the system regarding I don't know cyber hacking or.  Just that it it didn't work appropriately.  I think that would lead to a cascade failure to more.  A services or. | | |
|  |  | P24 |  | Components of society. | | |
|  |  | P5 |  | Air gapping is good and that is a security control that I would recommend.  However, we do have to move data eventually somehow through flash drives through supply chain you replace a part.  How good is the part that's coming in?  Did you check?  Maybe it has malware on it that comes in right?  Umm, there's lots of ways to bridge the air gap, but air gap is still one security control that you should probably should do if possible.  Yeah, it's a defense in-depth process. | | |
|  |  |
|  |  | P5 |  | Of course, of course, because now you're essentially connecting different functions together.  Through these networks and things like that, so that and also to gain access, you know original access, you might be way down at the very end, but if it's all connected, you just pivot your way through these systems that we have proven over and over again to get to the final system of interest.  So yeah, interconnected. | | |
|  |  |
|  |  | P6 |  | So in old days I had to travel 2000 kilometres and then I had to even. It was a week.  It has sound a big ball and my God was just.  About the name I border, I have the. How do you call them all around the around the land? | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 56 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | Then we are in the supply chain. The supplier has to do it after responsibility for data and so on.  Nevertheless, the system becomes very complex and I think compared to 100 years ago, or even, I would say 20 years ago, the time that there is one engineer which understands completely and can describe his system, it's gone even without AI. So it has nothing to do with AI. It's gone. It's overall unbelievable, became complex and nobody can oversee it. The world system, when AI comes into this, into the game as models, even then even more, you can no longer that the Minister can describe it.  So we have an unbelievable or an an enormous growth in complexity that's that's a big threat on the system. And since it's about software development.  We will always have our vulnerabilities in there.  And when we now accept as a threat model that we can discuss about philosophical way of political systems and human beings, there are plenty of threats out there which we see every day now on on the TV, there are always other people from crime to terrorism to state actors which will use.  Those vulnerabilities in our great infrastructures that we have very complex systems. | | |
|  |  |
|  |  |
|  |  | P6 |  | Also, a very general statement.  It is true for any IT systems, but also of course also for critical infrastructures. | | |
|  |  | P6 |  | Due to the digitalization and connectivity.  And using services and all this stuff.  Any IT system becomes more complex, so we are increasing dramatically complexity. Of course we are outsourcing a large extent. So for the stakeholder becomes easier because I'm outsourcing it to a cloud provider to service provider of course. But outsourcing doesn't mean that I get rid of the security responsibility so. | | |
|  |  | P6 |  | A barrier. Yeah. So you have. Even if it's not the military barrier. But it was a barrier. But you have to do something physically to enter the system power plant or something. So it was always this physical protection out there and the effort to enter it was a digitalisation. We have lost this. We have just a virtual barrier. And this and 8 billion people have no access to it. Have the tools. So it's about scalability, scalability and the attack vector. | | |
|  |  | P9 |  | So I I do worry about that.  And then so we've got the you got the supply chain interpolation, we've got the data sort of spreading aspects and then it's just a straightforward complexity of management of these systems. So some complex systems are resilient because they are intrinsically failure resistant, anti fragile.  And some complex systems are prone to catastrophic collapse.  And you don't know which one you've got.  Until it happens. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 57 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Data - Encryption - Protection** |  | | | | | |
|
|  |  | P21 |  | Right. Got it. So so, so the two sorts of data we're talking about then are data about inventions or things that are assets you know?  You know, competitive assets in terms of of of technology and things that are.  Presumably things that would allow people to be manipulated and as they say things about.  Personal, sensitive personal data. If on a large scale, yes.  That actually is can be regarded. Ah, so we have got another sort of critical infrastructure.  Yes, you know, if I've if I've got a Jean bank about, you know, describing describing several million UK citizens, I have something that is pretty critical because. Yeah. | | |
|  |  |
|  |  | P21 |  | Yeah, you. Yeah. There is no sort of retrospective.  Mitigation that you can sort of take. | | |
|  |  | P21 |  | Yeah. So the one of the other papers that we published on this was on the the harms that result as a consequence of ransomware attack. And this is ransomware, but it could also be other encryption or intrusion based crime. So it could be broader than that.  And in our research, there was no indication that some of the data that's been harvested by cyber criminals and leaked on the dark net, there's.  Additional harm resulting as a consequence of that because.  Criminals might use that data for further criminal activities.  The fear is that if I'm a lawyer, I've suffered from lansomer attack and my my clients data has put on the dark net. They are then exorted and they become subject to further crime because of that.  In our research, there hasn't been evidence for any systematic exploitation of that data, primarily because cyber criminals don't have to, because they're money driven, they have easier ways to make money. It doesn't have to be that complicated.  And there's that amount of data that they harvest is also it will change. I think with AI and better and more computing and passive.  Do you? But it's quite an effort to sort that data to analyse that data to then turn it into something that you can use for further crime, right? So that amount of effort and storing that data in the 1st place and you have to pay for that and so on and so forth. Yeah, that is currently not being exploited to the extent that one might fear. But I think that is something that could very much change if there's different data analysis capabilities. | | |
|  |  |
|  |  |
|  |  |
|  |  | P21 |  | Or perhaps also the ability to, in retrospect, in retrospect, decrypt some of the data that's been harvested. | | |
|  |  | P21 |  | But I mean, you can also can also be less sophisticated, right? I mean, a lot of what we're seeing in this context isn't actually as sophisticated as as something like that. But by 2040, who knows? I mean, cyber criminals have been pretty inventive and pretty have welcomed new technologies with open arms to ensure that the business remains lucrative. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 58 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | To current event not decrypting, they are they're currently, they're not decrypting, they're encrypting, if anything. | | |
|  |  | P21 |  | And like you have to back file everything for 10 years and so on.  Greater education and awareness also on what data you can then delete and sort of good data.  Like it's there's harder, security, harder and good data hygiene as well. So I think that that's one aspect. The other thing that we've seen quite successful offensive cyber operation by UK and U.S. law enforcement agencies or the FBI or other institutions. So I think.  Taking taking ransomware as a all the encryption leaking of data as a as a security national security threat rather than just a crime.  For example, as well as with as well as the case with terrorism, that would be another example where it was then elevated to national security threat and you'd get all kinds of resources and and.  Skills and people and so on from the problem. So something like that, I think. I think really changing the narrative that our privacy and our data protection that that's a risk to national security and to democracy and society as we know it. I think that that would be a thing for change.  And then at let's see. | | |
|  |  |
|  |  |
|  |  | P21 |  | I mean that could be 1 version, right? That's highly that's highly context dependent whether the past actually responsible or not. But for example GDPR includes that you have to have GDPR training for your staff and so on. But most of the companies who have organisations that have data leaked are underway of what data they have in the business. So for example a greater awareness on can we also actually delete data that you no longer need. There's also sometimes organisations are under obligations to hold on to data. I don't know whether your tax. | | |
|  |  |
|  |  | P21 |  | I think in the UK particularly, we have debates about a new privacy law, right?  There's in the. I think the bill is is up for for signatures, so to speak, so.  The way we perceive data and data privacy, I think it's that's a an important national debate to be held and I think I I get it, it's quite a dry, boring topic at times and also it's quite easy to fall into the trap of thinking that all we want to be this AI superpower, we need more data. We need to be a bit looser on our data regulation. But I think long term the UK needs to realise that data protection is.  It's a national asset. It's a privacy is what makes a democracy.  So I think the importance of data protection because with all of these technologies, we always say, oh, new regulation and maybe we need a new law and so on. But so much of that comes back to data protection. You don't.  Your need for AI specific regulations, perhaps less the case. If you already have solid data protection laws in place that doesn't solve everything, but it's a pretty good starting point and I think in the UK we'll also need to. So it's it's that economy that like last data protection is good for the economy that I think it's a false false friend.  And the other bit is that there's been particularly around Brexit, quite a stark anti GDP R movement because.  Currently, the UK Privacy Laws EU branded right and that's undesirable in that context. So I think a certain reconciliation with that and realising that for example, the EU has been very successful on with its data protection and exporting that. And I think we should seek that. | | |
|  |  |
|  |  |
|  |  |
|  |  | P21 |  | Exactly I need to change my fingerprints right now. Yes. Yeah, exactly. Yes. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 59 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | So there are certain there are certain sorts of data that are actually.  What sort of data are you thinking of? That would be an actual threat to national security. Then what sort of thing is that?  OK. Yes, yes. | | |
|  |  | P21 |  | But or just leaking or exfoliating in the last place. But one could imagine a scenario where this, perhaps less on a criminal spectrum, more in an espionage spectrum where they're harvesting data that is encrypted.  They currently can't access, but in retrospect they might be able to access that by 2040 because by then they have the capability to decrypt. | | |
|  |  | P21 |  | Your biometric gene data, but then also also.  As far as the NCSC already provides cyber central training, I think would so that certification scheme for they help out umm tech companies. So I think if you think about emerging tech companies to make those safe.  And and increasingly secure. So it's data like highly personal data and then data of technology development and those disruptive critical technologies that are evolving think quantum AI capabilities or so on to also make those infrastructures particularly.  I'm secure. I think that's also a name. | | |
|  |  |
|  |  | P21 |  | If more of the the data that we've seen stolen for in ransomware attacks and other intrusion based crime or espionage, for example, if there was either ability to decrypt some of our data very respectively, or just analyse some of the unencrypted data that's been harvested, I think that would quite fundamentally change the ecosystem in which we in which I sort of look, I sort of look at in terms of.  Cyber crime.  Policy making. | | |
|  |  |
|  |  | P21 |  | Yeah, that can be. You can get a new one. Like if you can't easily get a new one, but if you really have to, you could get a new one, whereas your DNA date on your DNA and sort of other biometrics and that you can't change and.  It would sort of, yeah, quite worry me.  Who needs that kind of data? For what purposes? So I think there's different kinds of data that you need to protect. If it's A/C and I supplier that deals with something like that that I think would be quite quite worrying. | | |
|  |  |
|  |  | P21 |  | OK. But so so you see the stolen data and analysis of that with the aid of AI as being potentially something really quite.  You know, quite worrying. | | |
|  |  | P21 |  | Yeah, I think there is a lot, a lot more data out there than we currently assume. This is by the darknet, but also commercially available data. I think it's quite.  Daunting at times, how much data is out there? We don't. We don't quite grasp, but particularly how much information that data.  Turns into if you overlap certain data sets.  And I think that our ability to really.  Use. The data will increase because at some point it will be more about the quality of the data rather than the quantity, and I suspect there may forthcoming technologies will enable us to to sort of make use of equality alternative to something qualitative rather than just relying on on everything that's publicly out there right now. | | |
|  |  |
|  |  | P21 |  | I do you some? I. Yes. National security number. Yeah. Yeah, yeah. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 60 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | So I think you can turn what we'd sort of now think of as more of an indirect victim. So not the past, who's actually suffered the ransomware attack by the person who whose data has been leaked. And all of us by now will have gotten emails from capital. I don't know whom, that our pension date has for leaders of health. I think it could could expand the notion of who's a victim. And then in turn, those who've previously been indirect victims, they could be turned to direct victims because they might then face crime fraud or something else.  As a result. So that would mean psychological, financial, reputational harm on them again. So it's really expands the the notion of who can be a victim. | | |
|  |  |
|  |  | P21 |  | If your pension number is being stolen or your.  What's it called? Your national security, not your national.  What's the number code that you're? Yeah. | | |
|  |  | P21 |  | Extortion, some ransom and theory assumes that you encrypt something, but you gross just blackmail without encrypting something. Just say, OK, I'm threatening to leak that data.  But I also think.  Industrial espionage, perhaps. | | |
|  |  | P21 |  | And the focus, as I said right now, criminals can still make money easily elsewhere, so. | | |
|  |  | P21 |  | A very difficult to quantify out, no, I don't think that's that. It's a bit coming up with something that's previously unheard of. I think it's just the the scale and scope might change, yeah. | | |
|  |  | P22 |  | Well, it's it's connectivity.  But the the.  No, I can't use the phrase in the wood part, but the the lurking danger that xxx always brings out is that so much critical national infrastructure is built has legacy systems in and they were built to certain standards in terms of, you know, data checking at the front end. And you know now they're being bolted on with lots of add-ons that are brought in from all over the place.  A lot of those systems do not have the same extent of verification of data quality at the front end, and that in fact is the source of a lot of cyber attacks that you know the data checking at the front end isn't happening. And you know there are components built into all sorts of devices that are used in critical national infrastructure that have known vulnerabilities that have been.  In the software.  Incorporates into 260 manufacturers, devices and are now 20 years old and are still there, so there are lots of devices with built in known vulnerabilities, but you know it's not a priority to sort of pull them out because they're working OK, hence the need for AI to record and analyse transient almost failures.  Because we know that there are these buggy devices, these vulnerable devices, these faulty devices in there operating, you know almost 100% but not quite.  And also subject to cyber attacks, because you know, if you've got good enough defences at the front end, the cyber, the, you know, malignant attacks. Sorry, I'm. | | |
|  |  |
|  |  |
|  |  |
|  |  | P22 |  | So there is a framework for actually narrowing failures. Now. If you talk to xxx, she'll say that's such a crude thing. She'll want all sorts of other things, but actually it's a start. If you can persuade governments to.  On it and even start with, not just trying to influence regulations to influence infrastructure companies, etc. But if government started to publish their own data, that would provide a role model and it would allow people not to feel guilty about software. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 61 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Decentralisation of services** |  | | | | | |
|
|  |  | P10R2 |  | Those sorts of things, and it's easy to see particularly, you know those those, those boutique style, you know, nuclear reactors. I just want to shout every time I read or hear someone banging on about, you know, boutique bloody nuclear reactors.  Should not be a thing.  Yeah, yeah. | | |
|  |  | P10R2 |  | Yeah, I can't exactly. What was I thinking there? Yeah, I'm. I'm particularly around around around CNI.  What tell you more?  This this I I don't see that fragmentation in in around cnis bring a good thing and again this this I'm probably coming across as as as as as as quietly Marxist here but I don't think that I think that that decentralisation you know aligns with the commercialisation approach and.  I think I I do. I do think that some, some, some sort of central court, central coordination and kind of oversight is, is derosa safety critical in this space?  Yeah, I again, I think there's a political element to that decentralisation mode. Dare I mentioned railways. | | |
|  |  |
|  |  | P10R2 |  | For example, so is that there is there is a case for this in the future being being so, but I and given how you know the water is also, you know, part of this this kind of sea and I-1 would think. | | |
|  |  | P10R2 |  | Yeah. No, I really don't. I really don't. I really don't think so. I just think that the, the, the costs are too high, the risks are too high. I don't see the incentive base. There's a lot of easier ways to make a lot of money.  The yeah. So I I really don't. The the only cynically in terms of it happening we we've seen external investment. So I do think this would be aligned and actually inextricable from commercialisation and and external investment and we've seen just looking at the kind of the kind of the geopolitical economic position we've seen how keen.  You know, sort of foreign, you know, nations have been and and, you know, big corporations in investing in things like water. | | |
|  |  |
|  |  | P10R2 |  | OK, so there's a should, but this was a. This was a forecast so. So there's an element of. Will this happen whether we like it or not? Yes. | | |
|  |  | P10R2 |  | But yeah, but I I I I think as I say in this case. So. So there I think the the it's an attractive investment proposition.  Because it's something that the government can't can't allow to fail. So if you can strip as much as you like out and then they go, of course they're going to pick up the pieces, right, because it's it's like, so, so there it that that is that is one you know mode informing my my kind of future you know forecast here but I still think the risks you know any sensible kind of investment and of course there are unsensible but it it's you know it's selling that to a board you know and we haven't seen any of the big you know the big tech Bros.  Seeing this as as as something that they want to want to to jump into either so that as part of the the imaginary, the culture, the narrative, it's not something that that that seems attractive. So that that's my thinking behind the strong you disagree there. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 62 of 316 |  |
|  | | | | | | |
|  |  | P12R2 |  | Decentralisation will enable decentralisation, operation delivery. Gosh, I hope so. But I kind of doubt it. I'm going to say somewhat disagree, unfortunately. | | |
|  |  | P13R2 |  | And and whether actually there there's something that could be even decentralised if you think about the waste management aspects of it, it's just something that's very difficult to do on a small scale, lots and lots of times. | | |
|  |  | P13R2 |  | The decentralisation of nuclear reactors or electricity generation. Well, maybe it's really the nuclear reactors. I mean, clearly, if you look at electricity generation technologies such as wind and solar, that they are quite dispersed and decentralised already. But but I'm not less convinced around a small nuclear reactors think. | | |
|  |  | P13R2 |  | I I I'm not convinced that.  Remote Communications will enable. | | |
|  |  | P15 Comments extracted |  | This is important because there will be more sites contributing to CNI but each may be less individually critical. | | |
|  |  | P15R2 |  | Oh yes, so the decentralisation of services. And again, I don't know if this is the reason I'm sort of adding in this extra detail because I don't know if you've got it. You might already have it and just think that's not the key point. But if you're distributing all of these things, you're not basically managing all of your like.  Eggs in one basket. You've got little eggs all over the place, and so individually, they're probably less at risk because if you take out one small reactor and you've got 100 versus you've only got 20 big ones, then they will be individually less important, but collectively still important. And then then you need to look at how do you understand the risk across all of them and how they function together? | | |
|  |  |
|  |  | P16R2 |  | Interesting. So not decentralisation in the way the Internet is decentralised, that will be there will be central hubs that we can't get, that that, yeah, could fail. | | |
|  |  | P16R2 |  | Yes, yes.  Yeah. So services will remain very centralised in my opinion. | | |
|  |  | P16R2 |  | Very, very centralised and consolidated in in in practise. So that's why I didn't really agree. I think that we will not see decentralisation. We will see a consolid consolidation around Microsoft and Amazon and.  A handful of companies, even though we could technically technically have decentralisation. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 63 of 316 |  |
|  | | | | | | |
|  |  | P16R2 |  | Capital and.  The real provision of infrastructure, so you know the the the gas farm and the and the and the and the big Chinese handful of providers. So yes, on paper the architecture seems very prone to decentralisation, but I think that and that's what's what we're seeing with AI and consolidation of AI companies and entities into a handful of companies. It's just a confirmation in my view that decentralisation on paper, but very. | | |
|  |  | P16R2 |  | Yeah. Yeah, this. Yeah. Disagree because I think. Yeah. So technically and that's what we thought about the Internet from the very beginning, inception of the Internet, you know, it's gonna be this beautiful decentralised infrastructure that's gonna be helping all of us access and share and well in the end, technically, yes. It's a distributed system, but.  Network laws mean that it's actually very, very centralised in terms of. | | |
|  |  | P17R2 |  | you disagree about decentralisation? | | |
|  |  | P17R2 |  | Yeah, I think.  Think about why I said that.  Yeah.  I think, yeah, I I don't think we'll get into this kind of distributed.  System of of of C and I assets. As such, I still think Core C and I will be very centralised. It will be very sort of Island Air gaps and that's that's a mentality approach and I think we've not changed the mentality today. So I don't think in. | | |
|  |  |
|  |  | P17R2 |  | What 2015 years time will will necessarily change that mentality. So I still think things will be very sort of centralised and and and worked around that I think. | | |
|  |  | P17R2 |  | Yeah, if we're worried about it, we centralise it kind of thing, yeah. | | |
|  |  | P17R2 |  | Yeah, I've not sort of.  I think, OK. I guess my argument's more to do with most things most what we call cnis as it stands today, Brownfield because it's a mix of some stuff that's new, but mostly it's old green going forward with Greenfield maybe not in 15 years but maybe in 50 years not in my lifetime potentially. | | |
|  |  | P17R2 |  | It's. Yeah, it's a go to kind of approach really it's. | | |
|  |  | P20R2 |  | And the other one, decentralisation of services, I guess.  You know, I think that there will be some pushback to things like small nuclear reactors from, you know, for for safety and security reasons.  I think if you're talking about the dispersal of functions like electricity generation.  You know, can that be done in a safe and secure way that guarantees the supply in the same way that it is now?  Or has there was the same resilience? So I think that again I I'm not totally sold on that statement that there are obstacles and challenges to doing. What's being assumed here. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 64 of 316 |  |
|  | | | | | | |
|  |  | P5R2 |  | This one I don't know as much about the decentralisation. The only thing I can say on that is I know that what we call Edge devices in the physical protection world or sensors in the Inc world, they are getting smarter and smarter every day. And so I think it is moving from that centralised place server type thing more out into the field devices. They're doing more and more of themselves.  And just transmitting information back.  Not as as much so in the old days it just was dumb information from the field out to a controller and but they're getting much more smart and they got a whole bunch more information that they're sending and controlling locally.  So I would probably say yes, I don't know how far if I need to go all the way or not.  But we definitely see the trend is that is that what we're talking about what I said. | | |
|  |  |
|  |  | P5R2 |  | Yeah, it all goes in there as well because I'm also working on small nuclear reactors with vendors and looking at their designs.  However, on small modular reactors, because they're gonna be a more of a first of a kind, they're a little bit defensive. They don't want to go full out. So again, I think that right here fits pretty well even for SM, Rs or small nuclear reactors. | | |
|  |  | P7R2 |  | Centralization of servicing.  Yeah.  I likely though the SNR or we we call them SMR small modular reactors, but yes, very good. | | |
|  |  | P7R2 |  | Well, Rolls Royce is pretty much into them. | | |
|  |  | P7R2 |  | Yes, someone, someone, someone told me. No, that's not a thing. And then I saw in the newspaper yesterday that Carlisle is planning to host a factory for them. | | |
|  |  | P8R2 |  | Yeah, the wording, the wording can be improved. Definitely, yes, yeah. | | |
|  |  | P8R2 |  | Yeah. I mean, yeah, do you know what after here I was about to say yes and now you put the small nuclear reactors there. You're little bit lost me here. OK. There's OK. So I just say someone. Look, I'm not disagreeing. OK. | | |
|  |  | P8R2 |  | Small reactors because you mentioned this, I could say somewhat agree. | | |
|  |  | P8R2 |  | . So we can, we can talk about a bit more if you like. I do agree, but I think it's a bit, it can be improved that particular standard, but I I finished, yeah, I mean like I appreciate is other progress, the sentence right up. You don't. Yeah. Yeah, OK. But it decentralisation. A good point, yeah. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 65 of 316 |  |
|  | | | | | | |
|  |  | P8R2 |  | Yeah, especially railways here, the remote communication, wireless radio. | | |
|  |  | P9R2 |  | Yes, there's so much in that statement that some of the bits I can, I can say I think they're going to be very good. I'm not sure about the small nuclear reactors. | | |
|  |  | P9R2 |  | Generally, if that makes sense, yeah. | | |
|  |  | P9R2 |  | And that sort of undermines the clarity of the of the statement, but there will be dispersion of electricity generation definitely. | | |
|  |  | P9R2 |  | I don't think that's as a result of revoked communication and wireless.  I'm not sure that that's relevant, so there's bits in there that I go. Yes, I agree with and there's bits where I go, that's a bit of a non sequitur. So I suppose, agree I I agree. | | |
|  | | | | | | |
| **Decentralisation of Services** |  | | | | | |
|
|  |  | P14 |  | this might be good rather than a bad thing. Are we going to be seeing a?  Decentralisation of the delivery of.  And the operation of some CNI services.  The first thought I had was around.  Electricity. So I think we're going to be seeing. I hope we're going to be seeing the proliferation of micro nuclear generators.  An even more micro level. | | |
|  |  |
|  |  | P14 |  | For decades I've been banging on about the value of fuel cells, and there are now some.  Companies that offer you to install a fuel cell in your home.  To take gas to generate electricity for your home and then to put that electricity into the National Grid. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 66 of 316 |  |
|  | | | | | | |
|  |  | P15 |  | , if the ways in which they deliver those services changes.  Although those services are being are changing.  That is going to be different. So I would say that particularly around energy provision, if everybody goes to solar power and you're much more on a sort of hyperlocal thing, then the way that you would manage that critical national infrastructure needs to change accordingly because the ways that people are interacting with those systems and the the mechanisms for getting them back online or or doing any maintenance of them or whatever it is.  Or the impacts change because actually I don't know if everybody had their own solar power system and a battery and and then the network went out. Well, actually everybody's got a battery. So you've got a certain window of time. | | |
|  |  |
|  |  | P15 |  | And anything I would suggest, anything where you've got a huge amount of infrastructure which needs to have surveillance on it. And I don't know around nuclear sites, if you don't have exonomy, you've only got X number of cameras and X number of.  CNC the civil nuclear Constabulary. They can only be in certain places at certain times. Therefore, like how well see you. Are you managing the the security?  You know, security awareness.  And situational awareness around risks that are physically present at the time and also virtually present and things like that. So.  I think again there are opportunities, | | |
|  |  |
|  |  | P15 |  | AI system has got programmed in to be able to recognise people's facial expressions but it reads them wrong, then it could lead you to make similar bad decisions. And so it depends on the algorithms and processes and things that are going into doing. If if we are basically substituting human human like interpretation of data with with a mechan like an automated system.  Somebody has to have built that and has to have built in what those things then mean and how to interpret them.  And that then brings into it a lot of its own issues. I think it also kind of it does also have like clear benefits around sort of security management for CNI sites where they'll be very vulnerable sites that will be wanted to will be wanting to protect. So there should be benefits and opportunities around that kind of thing as well. | | |
|  |  |
|  |  | P17 |  | For many, many years we've, we've we've kind of relied on a very sort of centralised system. You know, everything's kind of, you know, all your it centralised, you know, all our systems looking after retail or food chain, food supply chain, you know, very centralised in that manner. You know, you have big kind of groups that look after all and we're sort of seeing a sort of movement I think which is now decent decentralising it because you've got enough capacity and intelligence to probably work it on a node basis and let that node handle.  The paradigm shift at the moment. | | |
|  |  |
|  |  | P18 |  | There are people out there looking at the feasibility of using things like nuclear as a green energy source.  That's specifically developed for data centres.  How feasible of that is? I don't know. But you know that's that's an example of the steps that some people are going to to try and, you know, accommodate that growth of data. | | |
|  |  | P3 |  | And then it delivered to site and then put together constructed so that that kind of IKEA flat pack type. | | |
|  |  | P3 |  | And then the sort of really interesting thing I think is around, uh, new nuclear designs.  So there's this.  So that UK is governed putting a lot of money into and everywhere actually sort of these.  Sort of so called small Montreal small modular reactors, SMS and MICROREACTORS and advanced reactors.  And I think the advanced reactor really comes down to the idea around the type of fuels that they're using. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 67 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | So this kind of like changing the safety setup, changing the way that we want to operate these nuclear facilities, some of the applications of them and stuff kind of allows or invites or requires us to start to use kind of new digital technologies and by and we're sort of at the stage where it feels to me like the sector is sort of.  I mean, yeah, sort of trying out ideas. | | |
|  |  | P3 |  | SMR is sort of prefabricated if you like off site by a manufacturer, let's say General Electric or Rolls Royce or whoever it is. | | |
|  |  | P3 |  | And I think sort of enabled by this change in the safety kind of set up is allow them to be kind of remotely operated or have multiple modules upgraded perhaps by 1 control room. | | |
|  |  | P3 |  | that the sort of safety equation with these things is sort of changed quite significantly in terms of the nuclear design in the sense that if it's not actively controlled, it's sort of self cools, right? | | |
|  |  | P3 |  | Yeah, to to, to power.  I don't know a city.  Something with a larger footprint, but for example microreactors the the kind of idea is that they might set on the back of a truck.  So these things could be mobile, yeah | | |
|  |  | P5 |  | , I definitely am coming from more of a nuclear background right now because I've just been at the last ten years or so.  UM, I you know, there's a lot of.  So in nuclear, I'm involved in a lot of advanced reactor research with small module reactors, microreactors, things like that. | | |
|  |  | P5 |  | for me the biggest one that's more immediate is the remote communications because when you have multiple SMR's in a geographic area, they're talking about having maybe one control room that feeds to all of these reactors. | | |
|  | | | | | | |
| **Democratisation - upskilling** |  | | | | | |
|
|  |  | P16 |  | I give giving a Ferrari as a first car to someone who just like to an 18 year old full of testosterone, who's just had their driver's licence. You know, it's not a good that's there is a reason why we give second hand cars. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 68 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | To young people when they start out, you know very often, you know, we don't care too much if they scrap them and you know that we we ensure that they're not too fast and they're not too. So. So that it. That's the kind of analogy, you know, giving a Ferrari or a Porsche to someone who's just had their driver's licence. Usually it's not a very good mix. | | |
|  |  | P16 |  | The other one is that those tools are gonna be so powerful, but they're gonna still be used by very sometimes.  Unskilled people. So, and that's you know that. So that's what we see with Aiai benefit in general. And now I'm I'm thinking I'm talking in general AI benefits the most to the to the more unskilled and the more junior people because it enables them to make such a high jump in quality. But if you're an expert already, if you're a very expert hacker or very skilled hacker, I don't think AI is gonna make your life.  So, so much better. But if you're a script kiddie, or someone who starts out in hacking, it's gonna give you super powers that you may have no way of control being able to control. So. So I think that, you know, this kind of out of.  Crisis might come from a very skilled attacker not understanding fully grasping the complexity of the system and then not being able to control their attack, but also from the fact.  But very, very unskilled actors are gonna have access to super powerful tools.  That are gonna be sold to them by those mid level.  Hacking organisations or networks and who knows what they're gonna be using those for? I mean, I study hackers and most of them they're very young, quite immature, very impulsive. | | |
|  |  |
|  |  |
|  |  | P17 |  | One of the benefits of AI or Gen AI should I call it is you can you can upskill people who don't have skills if that makes sense. So you know, I mean I can write, I can write software code that's not a problem, But I'm I'm not the best coder in the world, but I can. I can write quite a few languages.  Some better than others, but if you don't know how to write code, you can generate code quite happily. You could probably build a fully functioning application that otherwise without Jena and AI you wouldn't be able to do at all. So when you then throw that on the opposite side of the fence and we're already starting to see this and it's it's all been predicted as well, a lot of things like, you know, the sort of attack vectors that we're starting to see are starting to use more clever, sophisticated ways and use an AI to sort of help generate.  More sophisticated code sets.  Obfuscation and so forth. So I think that's only going to increase when you look at the attack vectors that are there today and how AI can influence that. I think that will obviously add a massive technical advancement in that area, which will mean that making attacks will be a lot easier from from that side of the fence. | | |
|  |  |
|  |  |
|  |  | P23 |  | So there's there's all these reasons to think that cyber could be defense dominant, but on the other hand, I think the, the, the kind of technical thing, the technical challenge we're facing now is that it's becoming easier and easier to become an attacker. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 69 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Democratisation of Attacker Tools** |  | | | | | |
|
|  |  | P14 |  | with Ji and ML does offer combined with an Internet of Things which allows everything to be joined up in a. | | |
|  |  | P14 |  | it could be that hitting.  Wembley on the day of the FA Cup final would be far more significant, at least in political terms and in terms of the impact and keeping people awake at night than hitting a major power generator, which is part of the infrastructure. | | |
|  |  | P14 |  | there is now the what we were hearing from some of the experts is you're seeing I used that phrase before, the democratisation of some of the capabilities that could be used as electromagnetic pulse devices. Once Upon a time, there are the sorts of things that states could get access to and, you know, at the minimal end of the stage, you just get the white van man doing something stupid. | | |
|  |  | P14 |  | Passed away than ever has been possible before. You suddenly have an attack arena which is vast and with huge numbers of unidentified potential threats in terms of players who can get into that attack arena, you've got some interesting challenges there. | | |
|  |  | P14 |  | You've got huge challenges there, so when you get the democratisation of technology | | |
|  |  | P16 |  | The other one is that those tools are gonna be so powerful, but they're gonna still be used by very sometimes.  Unskilled people. So, and that's you know that. So that's what we see with Aiai benefit in general. And now I'm I'm thinking I'm talking in general AI benefits the most to the to the more unskilled and the more junior people because it enables them to make such a high jump in quality. But if you're an expert already, if you're a very expert hacker or very skilled hacker, I don't think AI is gonna make your life.  So, so much better. But if you're a script kiddie, or someone who starts out in hacking, it's gonna give you super powers that you may have no way of control being able to control. So. So I think that, you know, this kind of out of.  Crisis might come from a very skilled attacker not understanding fully grasping the complexity of the system and then not being able to control their attack, but also from the fact.  But very, very unskilled actors are gonna have access to super powerful tools.  That are gonna be sold to them by those mid level.  Hacking organisations or networks and who knows what they're gonna be using those for? I mean, I study hackers and most of them they're very young, quite immature, very impulsive. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 70 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | I give giving a Ferrari as a first car to someone who just like to an 18 year old full of testosterone, who's just had their driver's licence. You know, it's not a good that's there is a reason why we give second hand cars. | | |
|  |  | P16 |  | Because the tool they have at their disposal has some level of, I wouldn't say consciousness, but has some level of autonomy and automation that will actually that makes it.  Do things at a scale that.  An untrained or unskilled mind cannot comprehend.  So they just see, you know, a machine able to.  Achieve certain things, but without fully comprehending that how it it it's doing that and then they're not understanding the all the all the implications of their request in terms of.  Neutralising or harming the whole you know the the the targets systems. | | |
|  |  |
|  |  | P6 |  | What we have or the biggest threat what we have is the democratisation of technology.  I would call it that way so that what I mean Amit, is that that what we are we have been driving the last 30 years as a as the Holy Grail, everybody will have access. Everybody has can use the tools. That's advantage of the Internet.  And the smartphone, that's fine. So I'm not, that's that's no statement against it. So that was the positive innovation side. That was part of it about 30 years supporting this. So that was the, the, I would say the, the, the positive effect we built on our digitalization programme to develop and be provided to about that tool. So innovation out there, every communication there, every everything came as we predicted it. But at the same time, something which we did.  We did not foresee.  Is especially when we talk now about AI, but it's also the smartphone already and all the tools out there.  These are now powerful attack tools for criminals and terrorists. | | |
|  |  |
|  |  |
|  |  | P6 |  | So every spy 20 years ago would love to have those tools which everybody has on his smartphone today. Everybody. It's unbelievable. I can find everything I can Google. It's it's I have remote access applications out there for free.  It's unbelievable. That's cool.  So of course, before I had a few people only which were able to damage something, but now we have 8 billion potential actors out there with easy train training material examples, downloading something so very easy. And if I extend that even to the market that I can buy attack tools and services even services and I have a low cost investment.  In a normal business, so the tech vector by every either crazy or criminal person in the world is so we get the new term I think, which is not a summary out of it, I would say.  The principal state the same, but the scalability change dramatically. | | |
|  |  |
|  |  | P6 |  | Tools are out there.  Which brings in principle.  Increase the threat. Unbelievable.  Combined now with when we come to the crime side with mechanisms like or or tools, I would say like the virtual currencies which are also out there for some reason, we can discuss it and then stock and then creating money and what is but the biggest effect from my side beside this normal virtual currency stuff is they solve the scalability problem for cyber crime.  I mean, all is ransomware out there. It's just for one reason. It's easy. You can now approach 1,000,000 potential customers and if only 1% of this 1,000,000 is reacting and then you have even you have not to invest in the I I I remember in telecom master the most expensive project for 10 years was the building project I have now for free a building platform, very cool place to an online transfer address. | | |
|  |  |
|  |  | P6 |  | we have the crime because very attractive. It's a business model issue. So many, many people are just talking. It's even though I would say no criminal, how is it called mood or so it's just a business way of thinking if I can do it, let's do it, I can that the risk is low. I'm just doing it to many more people can do, the driver will be crime, I earn some money | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 71 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | Exemplifies the amplification of of.  Scalability for providing criminal attacks just.  Attacking them. | | |
|  |  | P6 |  | We somehow somehow every human being is crazy. Doesn't many crazy people out there for whatever reason, political, religious, whatever it is they want to destroy something. And it's very easy without criminal motivation. That's another motivation. Call it.  Psychopathic. I don't know what the English name is. They want to build something and you can do it. You can provide harm. You can demonstrate the weakness, whatever your motivation is again and again.  Many people can do it, not just 100 spies, but because we have 100 states.  Thousands of people with a short training course. You can do it | | |
|  |  |
|  | | | | | | |
| **Digital Transformation - Digitalisation** |  | | | | | |
|
|  |  | P18 |  | So I go, I go 2 folds. Well, that's let's not limit it to. So first of all, there's increased digitisation.  And coming with increased digitization comes.  The difficulty in in getting diversity into into systems. So if you've got.  Have you got analogue systems and digital systems? You know by by design there's an obvious.  Diversity of approach between an analogue system and a digital system. If the if analogue systems no longer become available because of that increased amount of digitization, then you're losing that diversity and you end up. If you're not careful, being susceptible to things like cyber attack across multiple.  Platform. So we intended to be diverse.  Also things like again, other common mode failures so are things like solar storms.  You know, could the solar storm affect multiple digital systems? | | |
|  |  |
|  |  | P18 |  | Whereas if you know if you had analogue systems in there, they're lightly impact of a solar storm, probably still impact on the analogue system, but its impact will be different. So the diversity might enable you to be more protected from from something like a solar storm. You know that's just two examples of where that diversity is important and and one of the consequences of the shift towards digital.  Is that a lack of competency?  A lack of competency around analogue systems, so we no longer or we got a very much reduced capability in the UK for analogue electronics.  Because lots of training and stuff goes towards.  Digital. Yeah. Yeah, people coming out of degrees don't necessarily understand analogue electronics. They're mostly dealing with digital things. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 72 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | OK, so before we go on to that, that's that's sort of basic level of increased digitization, but we've also got things which exacerbated further. So going back to the previous question, there's also other things that exacerbate those issues. So things like artificial intelligence, where we where it's it's very difficult to understand what AI is going to be doing, you know, and how it does it.  And the increased.  Reliance on things like that for people to make decision making and the it's susceptibility to bias if it's not done correctly. So that's another example.  Then I don't know Internet of Things, that interconnectedness of the digital arena means that it's becomes easier for faults for Miss.  Miss operation of your faults within the system to propagate across multiple systems and you get multiple system failure as a consequence of that. So it's the interconnectedness that comes with digital as well, which also causes causes a risk. | | |
|  |  |
|  |  | P18 |  | Use of digital things is.  Is kind of exponential, you know.  The kind of quantity of data grows exponentially depending on on use then and that limits soon happens, so you know there are. There are people out there looking at the feasibility of using things like nuclear as a green energy source.  That's specifically developed for data centres.  How feasible of that is? I don't know. But you know that's that's an example of the steps that some people are going to to try and, you know, accommodate that growth of data. | | |
|  |  |
|  |  | P18 |  | Given the nature of like the dynamic nature of the kind of cyber world, whether you know just be updates or cybersecurity update needs, then you need a strong strategy in there to say that, OK, we'll only update when the.  I mean and and these things happen and how vulnerable does that make you in between, you know? So there's, I mean, these aren't these are new issues to to but they are but they're but they're issues that become more prevalent because of the increased use of digital.  Or the reliance rather than misuse of of digital systems, I mean, but digital systems on the on the opposite, are we going to be positive as well? Digital citizens on the opposite opposite side allow you a lot more information. They the diagnostics have got a lot more advanced. So you can try and identify or rather than try you can identify.  Where things may be going wrong.  Earlier and deal with it in a proactive way, so it's not, it's not all bad. You know, there's there's.  They can. They can do more complex functions in a simple or more cost effective way, so you know there's lots of benefits to them as well. | | |
|  |  |
|  |  |
|  |  | P3 |  | Telecommunications information and communications technology in general.  So that we can handle things like renewables, provide new energy services.  And that sort of stuff and and generally speaking, making the kind of infrastructure a little bit more open and interconnected than it perhaps previously was, right. | | |
|  |  | P3 |  | with the the kind of nuclear stuff and yeah, so as you as you know there's got broad.  Kind of drive towards digitalization right in in, in, in both of these areas, which probably takes different forms, which is why I kind of maybe bring that sort of distinction in a way, although probably maybe the technologies are very closely related.  So with the kind of smart grades, you know this idea that we're kind of introducing more. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 73 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | How to protect those systems?  In the ITOT world industry.  Power plants and all. All this stuff.  The software systems enhance data exchange systems for situational awareness systems for providing intervability between different responsibilities. Government, private cross-border all these subjects. So we're in the middle. Also in the defence sector for the I have to say also in the defence contact crisis and disaster management crossing the bridge between defence systems and activities and private fun. So there are plenty of things to do. That's the field.  Where we are involved.  We tried to come from the scientific side, but of course, since we are an applied research organisation, very soon we try to build prototypes, proof of concepts, demonstrators either to develop new solutions to solve a problem or to support a better understanding on how to use the system or currently we are discussing which I'm very proud of. We'll see whether we can achieve it, which is also critical infrastructure, the new media platform in the world of disinformation.  I'll be have some information, fake news and now we have all those elections and the question is, what is? What should the public system, the public authorities do? So there is a media they can do something. We have the private users, we have dedicate them, we can provide tools to the private users. The state can do it. The market can do it. We have to define regulators or other NGOs which are which have to be done now, which have to.  Have tools. | | |
|  |  |
|  |  |
|  |  |
|  |  | P6 |  | So how does these technologies change their way of working? How can we support the transformation digital transformation process, basically? And in this context from the application point of view, we are working in projects and in solutions.  Solutions for crisis and disaster management, border management.  Critical infrastructure protection from physical perspective surveillance system sensor systems, but very much from the cyber security side. | | |
|  |  | P6 |  | But we have to have all the means and and frameworks, laws and regulations that they can do something. So in this context I can I I think we need more than one hour. I can explain we have.  So I would say I'm in the middle exact. That's the reason I think I think it was xxx which recommended me that I have some views and experience. What does digitalisation mean in the public context and especially when we look more in this security oriented use cases, I would say. | | |
|  |  |
|  | | | | | | |
| **Digitization Increased** |  | | | | | |
|
|  |  | P10 |  | and the surveillance that's going to need to be put in place to monitor. | | |
|  |  | P10 |  | I suppose the infrastructure you talked about CNI earlier, the infrastructure is going to be necessary to achieve things like net zero targets. So I'm really conscious of the contradictions here. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 74 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | So first of all, there's increased digitisation. | | |
|  |  | P18 |  | these aren't these are new issues to to but they are but they're but they're issues that become more prevalent because of the increased use of digital.  Or the reliance rather than misuse of of digital systems, I mean, but digital systems on the on the opposite, are we going to be positive as well? Digital citizens on the opposite opposite side allow you a lot more information. They the diagnostics have got a lot more advanced. So you can try and identify or rather than try you can identify.  Where things may be going wrong.  Earlier and deal with it in a proactive way, so it's not, it's not all bad. You know, there's there's.  They can. They can do more complex functions in a simple or more cost effective way, so you know there's lots of benefits to them as well. | | |
|  |  |
|  |  | P22 |  | One was initially looking at the impact and coming up with fact that actually the economic impact of software failures already was at least equal to that of Rd traffic accidents as measured by the gft.  We also realised that for both technological and sociological reasons.  The impact and frequency of software failures causing service failures causing infrastructure failures was likely to increase both those trends because more people are using it for more things.  More people are dependent on electricity as part of infrastructure.  And the technology. | | |
|  |  |
|  |  | P24 |  | I also find it interesting learning about.  The impact of digitalization and software in improving the infrastructure sector and build environment in general because.  Sadly, this is an industry that hasn't deployed.  In software, as a digitalization, as much as other industries | | |
|  |  | P8 |  | It comes to rail to be perfect, honest.  The technology tend to move slow if I have to say sorry in terms of game change, I wouldn't call them game changers. I mean, you know, so there are a lot of signalling systems. There are a lot of like operational systems. So they are provided by different manufacturers. It actually can also mean so on and they are being used by the signallers and the technologies in there are already already like evolved over the years and due to the nature of the railways, I don't expect them to change them to change that much, although I expect them to get more automated. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 75 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Disconnect** |  | | | | | |
|
|  |  | P22 |  | But you know we have. So we have this big disconnect between people. You're familiar with it and understand the problems and people who are not familiar with it and don't have the vocabulary to understand it. And it's probably a vocabulary around systems thinking rather than it specifically, but certainly.  If, well, again, xxx was saying that which spent several hours in discussion with policy advisers in gsit, and they were really nice guys. You know, one of them had an MA in measure Portuguese mediat, I think, and seamlessly gsit policy advisor on supply chain software supply chain. And actually she turned out to be quite bright because she came to a workshop and she had actually got it. But.  I shouldn't be having to be teaching people about.  You know the others are. None of them had any sort of STEM education, OK. And so systems thinking is a bit difficult if you don't have any of that. And so this was saying, well, she happened to be having a meeting of her research groups. And between them they listed like 130 people across the various government departments they work with. Now, remember, she is focused on infrastructure. So this was transport, this was.  Probably Ofcom. I don't know. So the 130 people and none of the people that they were in contact with had shown background.  Now this is quite frightening because I think it's quite a big change. I mean, certainly people I knew with science backgrounds went into the civil service.  Maybe they've all mustered out. | | |
|  |  |
|  |  |
|  |  |
|  |  | P22 |  | They don't have a shared copy copy area anyway. Yes. Yes, yes. So you. You've actually identified 2 new skills here. There's first of all, there's the communication with finance and senior. And you've also identified the communication with purchasing and law and those are and these are both from the sound of it fairly critical and they are not things that you normally find in it people.  So you're asking something quite important. | | |
|  |  | P22 |  | You're dependent on boarding component. You get, you get no support from procurement, you get landed with impossible contracts, like if it breaks, it's your fault, not the suppliers fault. | | |
|  |  | P22 |  | Well, it's all part of more people being able to cope with it rather than saying purchasing contracts for it. It it is a big part of the purchasing world, so more people should be aware of it contracts rather than regarding just special, I think. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 76 of 316 |  |
|  | | | | | | |
|  |  | P22 |  | It it may be here, it may be a useful career path, you know.  That people want to go. So one time I did have an expert purchasing manager come in and do an IT job and.  He was quite good. He did have a purchasing attitude, which is very negative. Drive them down attitude so.  His his group, the groups who work for him, didn't like him because he was always ready. Why haven't you finished?  I wish bigger than we thought, which is sort of a bit sort of as it is.  And you know, so if you, if you come up the IT route, you know what questions to ask rather than why haven't you finished, you know, because that's not available question. | | |
|  |  |
|  |  | P22 |  | Since the landscape is changing and the role of it guys is changing.  In terms of what they need to be aware of and what their certainties and uncertainties are, and it puts a lot of emphasis on it, guys for being able to communicate those uncertainties to the budget holders and this is a big disconnect, it's a real problem. | | |
|  |  | P22 |  | So who's going to look at an it guys aren't good at reading contract?  Why should I be yourself? So it's a big job. And so some of the procurement people we talked to on the working groups were really concerned about this. But you know, again they were trying to find somebody who was aware enough of the problem to start talking about it. | | |
|  |  | P22 |  | Procurement doesn't have the capability of looking at software contracts. | | |
|  | | | | | | |
| **Disrupting Response to Attacks** |  | | | | | |
|
|  |  | P15 |  | The impact of them is going to be on your, on your systems, on your critical assets and on your processes that you're trying to protect and then using that information for situational awareness to realise when things are actually something is about to happen or something has happened and having an ability to recognise that and then using that situational awareness to inform your response. So being able to activate the right responders, being able to share information with the right partners and then to be able to sort of maintain that situation, that situation awareness as the incident is being responded to.  And then afterwards. So I think if you think about technology informing each of those different processes, I think.  There's a lot of opportunity, potentially both to do that badly.  For somebody with malicious intent to try and disrupt the information flow, so either to prevent you from knowing that something something is happening to be creating a risk.  In terms of cyber threats and things like that, but also to disrupt your ability to to collate information, I think there's also just a sort of not even from a malicious intent perspective. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 77 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | if you've got A and I'm just sorry that's able to manipulate your perception of the threat.  Ohe ohe be direct you, yeah, redirect you right to to to sort of, you know, to the wrong kind of, you know, to think about the wrong problems.  You know that that's a potential risk.  I mean, I can't think of any concrete scenarios, but you could imagine somebody trying to do that. | | |
|  |  |
|  | | | | | | |
| **Diversity in Systems** |  | | | | | |
|
|  |  | P18 |  | Whereas if you know if you had analogue systems in there, they're lightly impact of a solar storm, probably still impact on the analogue system, but its impact will be different. So the diversity might enable you to be more protected from from something like a solar storm. You know that's just two examples of where that diversity is important | | |
|  | | | | | | |
| **Economic Issues** |  | | | | | |
|
|  |  | P23 |  | I | | |
|  |  | P23 |  | See the if someone builds a performance quantum computer, there will be really diabolical attacks that one can make.  Umm, what we describe as the idea that of of not attacking an individual computer, but using one's resources to attack a software signing certificate or a website certificate.  And then all you have to do is get someone to visit that website or download the Microsoft update.  That would be that would be the attack right now.  We'll just, Steven, assuming that one had a quantum computer that would be a very, very, very expensive attack on on the order of millions of dollars.  I'm so for the foreseeable future, it's the cheap attacks and the cheap attack.  Umm, it's still fishing and so the the, the, the kind of the remediations that we need to do in the near future include things like multi factor authentication and what I see like in defense contractors is they do a lot of domain whitelisting and blacklisting.  So, you know, guess what? | | |
|  |  |
|  |  |
|  |  | P23 |  | You can't log in from Romania. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 78 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | Well, you know, if you think about sort of umm, you know operating some vendors you know you know there's this sort of you know operators maybe or regulators have certain requirements with respect to cybersecurity that are challenging and expensive to implement from a vendor point of view from a system integrators point of view.  And if you think about new query in particular, there are sort of.  It's not a particularly large market, right?  So if you're a vendor, you want to produce widgets that you can apply to as many markets as you can, so you don't want necessarily to be sort of tied down to very specific security requirements for market sector.  That's not huge.  There's attention.  There's like an economic tension. | | |
|  |  |
|  |  | P3 |  | Yeah, that's gotta somehow needs to be resolved in in the end. | | |
|  |  | P3 |  | You know what, we might call industry or the, you know, they're world outside of academia, be that regulators, vendors, operators, you know that Community needs to come together in some forum, right to to, to sort of get these.  And you know, this conflicts of interests in, in many cases, you know, there's that need to sort of be reconciled. | | |
|  |  | P3 |  | You know the price per kWh has to be attractive and everything that we've talked about doing makes it more expensive.  Perhaps for prohibitively so, yeah. | | |
|  |  | P6 |  | I would say with to the economic.  Barrier to invest a lot of building a bomb and travelling, but you don't need any kind of investment. Just by fun you can attack big systems. | | |
|  | | | | | | |
| **Education - training** |  | | | | | |
|
|  |  | P11 |  | My concern, and by the way I I don't quite know how much of your interest is in the adversarial actions against the CNI and how much is just about wizzy technology for building the CNI. But I'm I'm more more concerned with the the adversarial action because that's where I come from. That is my, my history, my background.  I see security is being taught too much as an additive activity.  An existing system design.  Particularly one that has been through all the safety processes and has been deemed to be, you know, just just fantastic, that's just excellent. So now with your security nodes, please do whatever it is you do, but don't touch our system because it's, you know, because it's fine now we want to put it online. So we you'll probably want to put some do some stuff around it. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 79 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | So where where is all of that thinking to bring it together in such a way that it sits in some kind of systems engineering?  From design.  Through construction and through operation. | | |
|  |  | P11 |  | Drawing all those. Yeah. Now, drawing all those threads together. What we're actually talking about is how do we make?  The critical infrastructure of the future, resilient not only, I think against.  Adversarial action.  But against failures.  And this is where.  We touch on probably my favourite favourite, my most vexed topic, which is the relationship between safety and security.  In assuring complex digital technology.  And I think this is this is the systems engineering thing that I wanted to. | | |
|  |  |
|  |  | P11 |  | My position is as a systems engineering problem because I think that it's.  The achievement of resilience.  In the face of adversarial action.  Or failures of of unusual nature because we don't have the history such As for weird types of censors or whatever.  Needs to be done in a different way than the manner in which we're currently teaching it. | | |
|  |  |
|  |  | P18 |  | Whereas if you know if you had analogue systems in there, they're lightly impact of a solar storm, probably still impact on the analogue system, but its impact will be different. So the diversity might enable you to be more protected from from something like a solar storm. You know that's just two examples of where that diversity is important and and one of the consequences of the shift towards digital.  Is that a lack of competency?  A lack of competency around analogue systems, so we no longer or we got a very much reduced capability in the UK for analogue electronics.  Because lots of training and stuff goes towards.  Digital. Yeah. Yeah, people coming out of degrees don't necessarily understand analogue electronics. They're mostly dealing with digital things. | | |
|  |  |
|  |  | P18 |  | Yeah. Suppose I suppose knowing maybe it maybe it's competency and awareness as well as behaviour, isn't it? Yeah, there's a risk that the technology and the assumptions around the technology can just take it, bring everyone with them. And that questioning attitude and the behaviour around it is insufficient to make sure that it's all being engineered correctly. So maybe it is Quant, maybe it's twofold.  Is competency.  And behaviours.  I've been doing some work with with IAA and International Atomic Energy Authority around competency and innovation.  And the model that we've come up with is for any application of stuff new.  You need three people.  You need a person who's competent in the technology.  You need a person whose competence in the application of that technology. So. | | |
|  |  |
|  |  | P18 |  | But this behaviour around that, isn't it? You know what's what's a bit. Well, I guess there's processes in there understanding threat actors and all that sort of stuff. But you know, if you've got the right behaviours around it, so which resulting in the right engineering.  You know the right levels of. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 80 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | More you know, experts in you know, whatever you wanted to apply it to and the third person you need is someone who's competent in the.  Process of implementing innovation.  So being that that kind of.  The precautionary principle, you know, knowing, knowing, kind of how you go through the process of developing technology readiness levels and you know the ways of mitigating risk because of that. And I think I think that stacks up an awful lot that between those 3.  Skill sets you can end up with effective deployments of some stuff new, but take any one of those three skill sets away. Then you're leaving yourself vulnerable to either.  Not going down a due process or not having the right level of information on the application or not having the right level of information on the technology itself. So I think that's that's a helpful model to think about.  Those behaviours and kind of competencies around the deployment of innovation. | | |
|  |  |
|  |  |
|  |  | P18 |  | Dealing with the consequences should a cyber attack happen, you know that that's that's about human behaviour and about making sure the adequate the processes are adequate. | | |
|  |  | P23 |  | Well, there there's definitely a Human.  There's a Human challenge, right?  All of our nations, I mean.  So many of my computer science students are Indian.  In Chinese, because even the US cannot produce the the number of people we need to understand programming and engineering.  So I think a big part of it is is Human investment.  I think another on the legal side.  Umm, we have a real problem in America. | | |
|  |  |
|  |  | P23 |  | Umm launched 1000 companies and Umm and so it it.  One of the things that's very scary is to see the world, not just, you know, you know, I think it was an Argentina.  Umm, where the new the new president has gotten rid of their Science Foundation.  And so on that the the world kind of reaction is is a very, uh, a scary thing. | | |
|  |  | P23 |  | I don't wanna go into it because it's not really your, your a the basis of your study, but there is a big attack in the US on how agencies regulate and the Supreme Court is very likely to make it harder for agencies to regulate.  And this is just obviously problematic in a in a world where we give we elementally let the private sector do the things that keeps us alive.  And if we can't rapidly the sheep that activity, I'm it with that.  So there is a there's a legal problem of agile regulatory, umm behavior and incentives that create agile regulatory response.  The I am I am really worried about in the US.  So those are those are some of the issues I I worry about.  I'm a big believer in government spending and basic science.  I think the US experience is that the space race. | | |
|  |  |
|  |  | P4 |  | So if if we know that a task is too difficult and a pilot or someone on the ground is gonna be overloaded, that's gonna have also all sorts of implications.  So the corollary of all this is that education actually matters from a certification point of view as well.  And one of the things that we are actually going to be looking at as part of my J job is what we can do to try and level.  I wouldn't, I say level up, but make sure that as as much as we've got all this technology coming along, we've actually got people that can actually engineer it. | | |
|  |  |
|  |  | P4 |  | When you say create the software, I mean we we're not just talking to people that are developing the software, we're talking about people that are gonna be evolving it, maintaining it.  I mean, we're talking about a plan.  We're talking about platforms here that will be around for maybe four or five decades, which actually and if you look at a lot of critical infrastructure, these are long lived systems. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 81 of 316 |  |
|  | | | | | | |
|  |  | P4 |  | Maybe what we should be calling ourselves, we should be calling what we call software engine is based is something that something like high integrity software engineering because people might not be passionate about building things for like water treatment systems, but they do want to build autonomous cars or drones and these sort of things.  And some of these things are actually high integrity systems because of what they do. | | |
|  |  | P4 |  | And you've got 120 credits in a degree.  You're gonna figure out pretty quickly that there's not gonna be enough credits.  College degree program so one of the concerns that the that certainly that I have and I think is shared by other people is whether as much as staff is advancing a big reverse salient here is actually software engineering knowledge.  And one of the things that worries us is less the technology but more our ability.  So if we're gonna, Sir.  The the work we did around Athens was motivated around the idea that all this novel technology is going to come along.  It could end up on an air platform, and it's gonna need to be certified.  Now if you look at software certification, it's not just about testing. | | |
|  |  |
|  |  | P4 |  | And and from what I know of the way universities work, it has to be pull rather than push because even if it university does offer lots of training in whatever it is that that we deem necessary, unless the students see it as being an essential part of, you know, a skill that they want to come out having, then they're not going to attend because we're not one of those countries, as you say, yes. | | |
|  |  | P4 |  | Forget specific variations of LLVM to indicate where there is how deeply it's gonna be looking at capability provenance.  There's a lot of knowledge there that is gonna be that's gonna be required at that.  The people aren't being taught at the moment because it's new technology, but it may well be that there's relate to technology around operating systems, compiled languages that people also aren't being taught, and that's uh, and that that's a worry to us. | | |
|  |  |
|  |  | P4 |  | So particular interest and and I think I I think I can say this because I've I've not just given talks on it, but we we we had a meeting with EPSRC last week and they agree it's issue as well, it's actually around.  So if you imagine all the all this future technology that's gonna come along and people are gonna sort of probe, are gonna program for.  And if you imagine that we've got a pipeline of people that have to have the ability, you know, come out of universities to sort of program and stuff.  If you imagine what an undergraduate learns at university, they will learn a discrete modular stuff.  That's sort of 20 credits. | | |
|  |  |
|  |  | P4 |  | So you'll you'll you'll probably know we put a we've put a the government put a lot of money into the whole Morello cherry program.  You know, this whole idea that we've got capabilities based hardware that's going to remove the notion of of memory based attacks.  Well, that's fine.  And that's that's important technology and it's useful technology.  But if we wanted to drop that into the ecosystem now, people are gonna have to know how to operate it.  Which means that if people are gonna have to rebuild software for that, they've gotta take a make file and run it and change the make file.  But where's are we confident that people have got the knowledge of of actually how to do that?  I mean forget changing compilers. | | |
|  |  |
|  |  | P4 |  | It it's not a unique problem to higher education, there is stuff that can be done to help.  We do know friendly primes.  We are looking at how we can feed the outputs from one project into other projects.  So there are things that we can do to help, but that Will's gonna be there.  It's not my job in government to tell you this is what you're gonna teach. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 82 of 316 |  |
|  | | | | | | |
|  |  | P4 |  | It's not just about verifying the software we care about validating the software.  We care about security and safety, and we all secure about whether the people operating it and maintaining it have sufficient knowledge. | | |
|  | | | | | | |
| **Electromagnetic storm** |  | | | | | |
|
|  |  | P11R2 |  | That's right, because we've never, we've never, never really experienced it. So that that was my reaction. I didn't know how to. I didn't know how to structure these risks and again, didn't quite.  Oh, I don't know. So I think a bigger risk, maybe a different question is what's missing.  The risk that.  Critical infrastructure.  Come a legitimate target for.  Activities.  Political rivalry or?  There's a there's some nice Latin words for it, but you know the the the point before you go to war. | | |
|  |  |
|  |  | P11R2 |  | Yeah, yeah. But whether it's major or just business as usual, who knows? Yes, yeah. | | |
|  |  | P11R2 |  | No, I strongly agree it's an issue, but I would put it in.  Low likelihood because.  I don't think people recognise yet the vulnerability, but it's a separate point, which is that the solar flare doing the same thing.  I mean, I think there's a much greater chance that at some point between now and then we'll we will experience some kind of so solar event.  Which will cause some form of disruption. | | |
|  |  |
|  |  | P11R2 |  | This has been a concern in some parts of the West for a very long time and I can I can tell you I could build if I put my mind to it.  A A small white bum, a large white van, sort of 1 1/2 tonne capacity white van.  As an electrical engineer, I would know how to produce an EMP device. Non nuclear EMP device that would destroy a lot of the front end PN junctions on.  Electronics. If I took that into the City of London. | | |
|  |  | P11R2 |  | But we've known this, we've known. So any engineer, if you ask them and the electrical engineer will tell you, you know how to, this can be done.  Just fortunately no. But maybe you don't need to write that down. | | |
|  |  | P14R2 |  | Which of course is one of mine. It's just only somewhat disagree because I know this is going to happen, but I can't say it's going to happen by 2040.  That's all.  I think this is a massive issue. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 83 of 316 |  |
|  | | | | | | |
|  |  | P14R2 |  | And that last one was in 1850, the last one was 1859. So then that would need one to say it's right to say there's a reasonable chance, but I don't think.  The the database the evidence base is sufficiently strong for you to be able to say that with any certainty.  So if there was somewhere between somewhat agree and strongly agree, I would be urgent leaning towards saying in between. | | |
|  |  | P14R2 |  | I'm 100% certain this is gonna cause real problems at some stage scale of the problems depends on what we've done to build resilience, and the timing is questionable uncertain. | | |
|  |  | P16R2 |  | But at the same time, it seems that we've never experienced such such an event.  We maybe we operate not on the same time scale as the as the storm as the sun system and we don't understand the odds or I do I do not understand the odds. I I think astronomers and physicists they do, but for me it's it was impossible to assess. | | |
|  |  | P16R2 |  | electromagnetic storm that that, that's where I. So I didn't know really. I I, I I've kept reading about it over the years. I understand the the, the the principles and and it could be a very, very catastrophic event for us. | | |
|  |  | P17R2 |  | That seems OK. It seems quite resilient in that sense.  And I think the way we've got connectivity today, I think I mean definition of electromatic storm is it like you know, is it an EMF generated in a in a in a site or you know if it's a nuclear bomb for example, obviously it generates an EMF. | | |
|  |  | P17R2 |  | And you're not convinced? Moving on down to an electromatic magnetic storm. | | |
|  |  | P17R2 |  | Solar flare from the sun, which which didn't take out the satellites. Obviously it had an effect on the RF communications with the satellites to to the Earth, and there were some over the over the air RF communication space. It was a bit disruptive, but I mean. | | |
|  |  | P17R2 |  | Outcome from from the from the blast radius. But I mean yes, that would obviously massively affect the target area.  But I think there'd probably be enough redundancy communications to sort of establish. And if you look at Ukraine and Russia raw at the moment and a lot of Ukraine's telecoms and national communications infrastructure was targeted at the very start of the war. But the use of things like Star link and new types of telecom telecommunication systems have allowed them to quickly mobilise, you know, communications probably not to a level that you'd want your country to be out. Like we we live in the UK at the moment, for example. | | |
|  |  |
|  |  | P17R2 |  | Why we've got multiple different avenues, but they've got, you know, communication streams that are both secure and and for general availability and you've got people still working in Ukraine that are not far from the from the war fronts and they're still on the Internet doing work, you know, remotely. So, yeah, I think there's enough evidence to suggest that there's probably quite a bit of resilience there, to be fair. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 84 of 316 |  |
|  | | | | | | |
|  |  | P17R2 |  | It's a tricky 1 because we just don't know what we don't know, do we? I mean, a good example of that was a couple of weeks ago where we had quite a significant. | | |
|  |  | P20R2 |  | Again, I mean, I just, I sort of I take issue a bit with that may destroy many vital components of modern infrastructure. I mean what is the scale you're referring to here? I mean I think it could lead to probably short term temporary outages. Is it going to just en mass take down infrastructure? I'm not entirely convinced, so I'll put somewhat disagree with that. | | |
|  |  | P24R2 |  | DNA in general, I I know that here you will explain.  Disabling power grids, communication systems and computer. But these things can be disrupted also by other extreme weather events. | | |
|  |  | P24R2 |  | I would change electromagnetic storm to.  Weather events in general.  Like extreme weather events, and one of those is the.  This one in particular for like. | | |
|  |  | P4R2 |  | No, no it it, it could happen. I don't think. I don't know about a reasonable chance of all the things that you describe though that it will destroy your components of modern infrastructure just because I think people, I mean people design hardware to be resistant to sort to sort of EM already. And I think I would like to hope that.  Because of that C and I operators are thinking about it too, so certainly in defence we think about it.  And I would like to think that others think about it as well. | | |
|  |  |
|  |  | P5R2 |  | We've been talking about Emps forever and it hasn't really materialised. I'm gonna stay neutral on this. I haven't heard anybody talk about this yet.  I don't know if somebody were to do this, if that would be similar to like a nuclear bomb where it's just not good for anybody. So I'm gonna be neutral on this. I don't know if it's gonna go up or down. | | |
|  |  | P7R2 |  | I don't believe it's fiction. I I there was an electromagnetic pulse of a century or so ago that that did a lot of damage at the time.  I various people have told me yes, but this isn't really, you know, this will cause sensible damage, but others.  You know, others just don't know particularly sort of a nuclear bomb somewhere innocuous that just happens to affect affect us. | | |
|  |  | P7R2 |  | Yeah, I haven't thought about the electromagnetic storm, to be honest. Is it? Is it?  I don't know is it is it fiction? I don't know. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 85 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Electromagnetic Storm** |  | | | | | |
|
|  |  | P14 |  | The current 11 was meant to be a one in 150 years and that was more than 100. That was more than 150 years ago.  And we're probably due another and that took out all the telegraphy of the world. There wasn't very much.  Let's talk it out.  And there's no.  Certainty that we are sufficiently robust and resilience with our systems that you wouldn't have some similar, very severe.  Impact. So that is the one. | | |
|  |  |
|  |  | P14 |  | That's major. OK, so a major solar storm. | | |
|  |  | P14 |  | So the Russians decide to detonate a tactical nuclear bomb over the Black Sea, just as a warning.  Not aiming to kill anybody.  But the knock on pulse effects travel thousands of miles and could be taking out all sorts of bits of kit and equipment.  Yeah, but it would just be to be massive. It would be massive. Maybe I didn't write it down, but it'll be in the notes somewhere.  Everything starts going wrong if you get a serious solar storm.  And you have a sufficiently you haven't sufficiently secured.  Your your your capabilities to deal with the geomagnetic effects. | | |
|  |  |
|  |  | P14 |  | Power across the globe.  Internet across the globe could be seriously affected, but if it was actually only in the UK, take out enough of the.  Electronic the other sort of net, the network, the electronics power, net grid network. | | |
|  |  | P14 |  | this will probably be a solar storm of the magnitude that caused the Carrington event in 184959. | | |
|  |  | P14 |  | But that was I just remember.  Thinking that was an extraordinary list of everything, as people were just sort of reflecting on what the hell goes wrong. The answer was some very serious stuff. Yeah, yeah, I've given a sense of it. Transport telling. It's the telecommunications because often radio TV, because all these sorts of signals have been that badly damaged. GPS goes out. | | |
|  |  | P15 |  | The same goes around things around severe space weather.  And the impacts of solar flares on on things and how you start to look at risks and how they would manifest themselves.  So how that could manifest itself, particularly within a particular infrastructure in in terms of like the rail industry of understanding cable, a lot of those risks would look similar. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 86 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | Also things like again, other common mode failures so are things like solar storms.  You know, could the solar storm affect multiple digital systems? | | |
|  | | | | | | |
| **Forms of Infrastructure becoming critical** |  | | | | | |
|
|  |  | P10 |  | So, alright, so so this is a thing to look out for is where the the software or the the availability of these systems becomes such that you don't have the resilience of the old systems anymore. And that's a more general problem, isn't it that? | | |
|  |  | P10 |  | Certainly I'm not sure about E retail. I think you know, I think we lost. Sorry. Yeah. I, it's funny, isn't it? I I I suppose we, I suppose it does become critical if everything's lost. If everything's shut down before we get there. So like, you know, I I still insist on using our local hardware store even though it costs a fortune. And I have to carry heavy things home just because I know that when it closes down because I've been on Amazon all the time, I'll be really sad.  But that's not going to be enough to keep it going, so I suppose it's I. I sort of commented from another direction. It's it's and I think this is legitimate as as a concern here, we're losing. We're losing resilience. So I sort of so I think re retail becomes critical. If it's eroded, the kind of the physical, let's say, retail infrastructure to the extent that there's nothing to to pick it up.  And that and that's true of, you know, you could think about kind of food supply, it's about us almost a supply chain question, isn't it? And various other modes just as we always find with something you know interferes with that kind of system. | | |
|  |  |
|  |  |
|  |  | P10 |  | Yeah, exactly. Yeah. What if you know, what if there's, you know, the all the job centres go down or or something, you know it's it's it's it'll. It'll just a glitch in the system and people don't get paid I think. Yeah. Yeah.  Exactly, yeah. | | |
|  |  | P10 |  | That they have, despite lots of varied news headlines, say they seem to be OK, but I think it's, you know, for example, what happens if something else, the banking sector or the, you know, the the Universal Credit payment system and you know how quickly do we do we get to rioting and and kind of, you know, civil unrest when an attack and it could be quite low level but if it takes out a system like that you know I think that they they sort of cascading effects. | | |
|  |  | P10 |  | Yeah, exactly. So, yes, this this kind of this tracks across you know multiple different sectors when the the kind of over the reliance on technology, yeah, just just kind of erodes that kind of physical backup. So when I can't get you know deliveries whatever is actually I don't have the shops to go to anymore, they're not there and the supply chain that's bringing in you know various of these can't get through you know whatever can't get through put passport control and and can't get past you know various get those are the sorts of things we just don't have those resilience.  Anymore, yeah. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 87 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | I don't think telecoms was ever.  White the same.  Although by the by telecoms is vital to the grid and your black start problem really gets difficult if telecoms loses power now, but anyway. | | |
|  |  | P11 |  | Yes, yes. Well, you and you mentioned cloud. I think the only one that I think has really joined the.  Electricity, water and and and arguably gas is is now the Internet and I can remember.  About 2008, there was a discussion in in policy circles in the in in London where I worked at the time about whether the access to the Internet would become a human right.  Touch, but I suspect he probably has or it should be by now. | | |
|  |  |
|  |  | P12 |  | Wow, I feel like, yeah, so Cdn's becoming critical infrastructure definitely is the biggest thing on my mind lately. Payment processors. So things like like the squares of the world becoming critical infrastructure. We could also talk about Twitter and X, although, you know, these days, it doesn't really seem like at one point I think like, you know, pre Musk, I would have said, oh, you know, Twitter's kind of a bit critical infrastructure because of the news. But somehow, you know, people have routed around that failure a little bit more. So it's it's not as much.  So I'm gonna go. I'm gonna stick with Cdns and payment processors like. Yeah, I feel like we talk. We we talk discuss that in pretty good detail at this point. Yeah. | | |
|  |  |
|  |  | P13 |  | I mean, I mean looking at in terms of healthcare?  And I suppose you can look at things like supply chains.  And if you think about how, for example, medication is supplied and distributed, that's critical part of infrastructure. Same with things that are like PPE, for example, when you saw that through COVID. So I think I think that the whole supply chain.  Across the NHS that keeps it functioning is probably, yes, critical. | | |
|  |  | P13 |  | But you know, I mean, we have seen these kinds of things destructed by protests. So I'm thinking back to the fuel protesters, we had one must be like 15 years ago now that actually brought supply chains.  Down and that was relatively easy and thing to do actually. I mean what they did was barricade a fuel fuel depot and the whole thing came to halt.  So there's that kind of thing.  Other things that might affect it is where these things are manufactured.  So if you look at so the Pharmaceutical industry, it's a global industry.  Manufacturing takes place in various different locations around the world. It could be political threats there. That meant actually, that could disrupt your supply chain. | | |
|  |  |
|  |  | P14 |  | So that what you're seeing is that from that point of view, I would argue that builds resilience, so. | | |
|  |  | P14 |  | And then back to our very early.  Conversation. It's not just the location, it's also the time so hitting Wembley.  Large most of the days of the year wouldn't matter at all hitting it and it's the FA Cup final might be hugely significant. | | |
|  |  | P14 |  | so we we have our CNI right now.  I don't have much.  To contribute here, other than to ask the question, this might be good rather than a bad thing. Are we going to be seeing a?  Decentralisation of the delivery of.  And the operation of some CNI services.  The first thought I had was around.  Electricity. So I think we're going to be seeing. I hope we're going to be seeing the proliferation of micro nuclear generators.  An even more micro level. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 88 of 316 |  |
|  | | | | | | |
|  |  | P14 |  | So there's somewhere out there is this is this recognition that iconic buildings, public places, places where the public gather, where there's an expectation they're going to be safe and secure, go about their everyday business need protecting.  Concert halls blah blah. | | |
|  |  | P14 |  | More and more things have been judged to be significant, nationally significant, and what I'm thinking about are public spaces and critical public spaces and sports arenas, concert halls and the like. Those areas in rather generic terms seem to be being swept up into the under the umbrella of critical national infrastructure to a degree.  I don't know if that's formally the case, but you've I've sensed that happening.  And so things like the what used to be the centre of the production of national infrastructure certainly started getting involved, as I recall, in worrying about arenas. Partly, I think because of the threat being seen back to our very beginning of our conversation, because it was judged that certain iconic buildings.  Carry a critical a national significance.  They then become woven into the idea of being part of the critical national infrastructure.  Muddle thinking, you might argue, but nevertheless it could be that hitting.  Wembley on the day of the FA Cup final would be far more significant, at least in political terms and in terms of the impact and keeping people awake at night than hitting a major power generator, which is part of the infrastructure. | | |
|  |  |
|  |  |
|  |  | P14 |  | Exactly. Exactly. Yeah. Yeah. So that's just a question hanging there and I don't know if I know that 5G and there's there going to be A6 GI, guess there's going to be a 6G.  You're dealing with smaller and smaller cells.  And delivering.  And managing messages.  So that is a decentralisation in a sense.  And does that build more resilience? I guess potentially it does, but I just just asking the question.  I'd begin to run out of ideas other other than what I've seen in the years where I've been.  Involved in sort of national security stuff, I think. | | |
|  |  |
|  |  | P14 |  | But it does change.  The map of what is critical in a sense right the the map of who is delivering critical services or is it? Is it actually? Because if, if, if everybody was delivering those critical services, perhaps they don't become critical anymore or something new becomes more critical. I don't know the way that the network delivers that stuff around. | | |
|  |  | P14 |  | For decades I've been banging on about the value of fuel cells, and there are now some.  Companies that offer you to install a fuel cell in your home.  To take gas to generate electricity for your home and then to put that electricity into the National Grid. | | |
|  |  | P15 |  | Things that would fall into that category, but I think it is because it's not.  Yeah, I think it's because of that reason, not that we've necessarily changed that. We want different critical things.  Although that people say might have decided. | | |
|  |  | P15 |  | Before things start to happen, so we need to think about that differently to actually everybody gets their electricity off a grid which runs off a power station and all of the power stations have gone down and we're going to be in on an operation Black Star and it's going to take us three weeks to get all of them back up and running again. And it's like systems for turning one and getting one started. And that empowers the other fight, like the other five in that empowers and all of those things. So, like, the way that they're all set up and the way that those.  Critical services.  Are delivered impacts.  Exactly what it is that what it means to be critical. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 89 of 316 |  |
|  | | | | | | |
|  |  | P15 |  | I'm not necessarily just on transport, so that if. Yeah. So yeah. So if if critical national infrastructure is critical, it is critical because not it's not just critical for the sake of it, it's critical because it is.  There it's it's infrastructure that is essential to the provision of essential services.  And therefore, if the ways in which they deliver those services changes.  Although those services are being are changing.  That is going to be different. So I would say that particularly around energy provision, if everybody goes to solar power and you're much more on a sort of hyperlocal thing, then the way that you would manage that critical national infrastructure needs to change accordingly because the ways that people are interacting with those systems and the the mechanisms for getting them back online or or doing any maintenance of them or whatever it is.  Or the impacts change because actually I don't know if everybody had their own solar power system and a battery and and then the network went out. Well, actually everybody's got a battery. So you've got a certain window of time. | | |
|  |  |
|  |  |
|  |  | P15 |  | No, but then that comes down to your definition of.  Of what it is that you're trying to achieve, and therefore if you like the things that we're trying to achieve haven't changed, I don't think we're just going about doing them in a different way than we might have done.  Before in terms of effectively like shopping.  A A physical shop on it. Opening its doors is important if that is how we do shopping.  Hmm, drivers and lorries and deliveries are important if that is how we do shopping and we don't go anywhere. So, so that the wanting to like the need for.  Like essential provisions hasn't changed. It's just we have changed how we do it and therefore.  The the things that become critical, they become critical because they're delivering a service.  So I don't know that I can identify off the top of my head immediately. | | |
|  |  |
|  |  | P16 |  | Yes. And I would, I would say more the cloud computing than the than any other sector, it's it's something I've actually.  Tackled in my work on cyber resilience with the banks because the so now for.  Economic reasons and cost efficiency reasons.  All organisations are using heavily, depending dependent on on cloud computing solutions. The problem is that when you have a financial so when you have a critical infrastructures are usually very heavily regulated.  And for a good reason, so that the regulators and the state ultimately want to ensure that they put in place systems to maintain high levels of reliability and we can have confidence in their ability to deliver critical services to to the population, what is not so heavily or so.  Meticulously regulated are those.  Cloud computing technologies, upon which those critical infrastructures more tend to rely more and more. So what we found is that the banks are very worried, for example about their.  Ability to guarantee that they will keep on being able to trade even during a crisis, because now they don't control. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 90 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | Computing systems directly anymore, but they rely on 3rd party providers.  Of which they know very little about, so it's easy for a bank to ask to see what's happening in the systems of their partner financial traders, because everyone has to abide by the same type of regulation, and so they trust each other. They know they have to operate, but then it's impossible to ask a financial partner institution to have access to their Microsoft.  Or IBM or Amazon cloud.  Services because those companies are much bigger and they say no, no, no, we just provide a service to you. Trust us. You know, we have thousands of engineers, so it's creating.  Lack of understanding of the the reliability and so the cloud computing. And now I think in the I think in the in the US the the the financial sector regulators are now asking submitting the cloud computing companies that service the financial sector.  To some high levels of oversight as well.  Saying that, if you want to enter this business with a financial.  Institutions, you're going to be part of the packet you're becoming part of the package now, so we're going to have to ensure that you deliver certain levels of services according to certain requirements. I think that the cloud computing, because it's introducing another layer of. | | |
|  |  |
|  |  |
|  |  | P16 |  | No. OK. So but yeah, but the legal sector, it's very interesting sector because it's not very tech savvy in the sense that usually.  Legal professionals. They tend to stick very much to tradition and to, but it's it's surprising how critical they are actually to the operations of the critical infrastructure sectors, because any company doing a merger and acquisition of another company has to.  Go through a a a a legal service provider that has access to their most important secrets. Their most important financial statements, and the legal sector, so holds the secret because of the cleaned you know the the the the attorney-client privilege and all of that. So they hold secrets.  The most important secrets of the biggest companies in the world, not not being very sophisticated at technology and keeping.  Under wrap, like the police or intelligence community. And so the the attackers are very knowledgeable of that and and and the target. And I know I know I speak of experience because I've acted as an expert witness in a number of cases that were never, never went to court because no one wants to hear about that or to air that kind of weaknesses but.  Those are cases of.  Billions of dollars in in, in fraud and secrets being stolen on the massive scale. So. | | |
|  |  |
|  |  |
|  |  | P17 |  | So this is edge sensors of various sorts within the infrastructure to yes. | | |
|  |  | P17 |  | Yeah. When? Yeah, things like, you know, you. If you look into.  Just just by looking into this, you know in the automation industry and the the highways, you know you got edge to edge like vehicle to vehicle, vehicle to person. So wearables, you know, talking to to cars basically.  Vehicle talking to infrastructure so the smart motorways, you got vehicle to vehicle. So car to car and you've also got vehicle to cloud and vehicle to telco SO45G. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 91 of 316 |  |
|  | | | | | | |
|  |  | P17 |  | So so the areas I guess, yeah, you kind of touched a bit on that actually with the cloud. So Cloud's virtual, it's a virtual platform hosted in data centre somewhere. So I think.  With the movement in the sort of digital twin space, there's there's a massive move there at the moment and it's really in its to early stages at the moment, but there's lots of funding and research going in that into that sort of space.  I think virtualisation of CNI is something that they're starting to to really sort of get on. I think I think that's where there's a movement to in terms of a technology sort of space because not to say that you can't necessarily replace something with a virtual kind of instance, but.  If you can kind of mimic or or twin it you know with a with a virtualization plane, which obviously does become part of the infrastructure because you need it connected at all times in order to give you real time monitoring and analysis and reproduction of the the modelling of that system. So I think that's something which is is probably not been given too much for at the moment this this kind of additional virtual play which will typically will be cloud based.  But I think that you know that effectively opens up your infrastructure and again becomes another form of well, it just widens the attack surface in my head at the moment.  Danny, the other aspect I think I sort of sort of touched on it sort of quite loosely, which was the IoT tech as well. So you know we're looking at at the moment, I mean like for example in construction, you know we're looking at concrete IoT sensors, you know which which you know are going to be these kind of almost these dumb pieces of sensors that you can read. If you put a thing near it, you know like an NFC sort of thing. But I mean if you start looking at things like that and drill down into the fret vectors.  You know, if you're relying on calculations from on a big bridge, which is a safety critical system, you know you you want a bridge to last couple 100 years. If it's, you know, reporting to you that you know that there are fatigues and stresses that are abnormal just because someone's been able to identify that it has sensors and they they rectify the signals it gives off, then obviously that might in, you know, implore a different solution that that, you know might might cause an unsafe situation or it might not. It might just, you know, 'cause.  And and unsatisfactory outcome. Basically, you know you've run, you find out that these sensors are wrong and you know you can't work on them basically. But I think it Edge is definitely a new area that I think CNI is just is going to embrace quite well. So I think that's an area that I think is is is you know somewhere to keep an eye on basically. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  | P17 |  | So you know, there's a lot more of that sort of starting to expand in in that particular area. And I think that would be the same for rail and maritime as well. So very much transportation sort of area. So there's definitely a lot more kind of edge sensor and edge computing which which is classified as IoT really. I think that's definitely an area that we're we're going to see more of a drive into as well. And I think if you sort of coupled that, even if you not necessarily C and I, but I mean you already start to see body tech you know like in you know.  Interjected chips and stuff like that into human bodies to interact with machines. So yeah, there's there's elements to that. I think that that that technology is is shifting towards basically.  It's a it's very much.  For many, many years we've, we've we've kind of relied on a very sort of centralised system. You know, everything's kind of, you know, all your it centralised, you know, all our systems looking after retail or food chain, food supply chain, you know, very centralised in that manner. You know, you have big kind of groups that look after all and we're sort of seeing a sort of movement I think which is now decent decentralising it because you've got enough capacity and intelligence to probably work it on a node basis and let that node handle.  The paradigm shift at the moment. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 92 of 316 |  |
|  | | | | | | |
|  |  | P19 |  | Thanks to the Internet, yes, operational technology is good discussed including the yeah, any kind of automated.  But yes, transport systems, yes.  Ohh, any of these is likely to be compromised if if if attackers have a will to do it.  And that is an increasing trend, doesn't it?  There's unfortunately it doesn't.  Yes, yes, yes.  And that the more the more computing, frankly that goes into the systems.  The more vulnerabilities potentially get introduced, yes, yes. | | |
|  |  |
|  |  | P20 |  | In security studies where we bigot, we begin to refer to more and more things as security issues and you know, is it really a security issue if someone's out of a job, do we really want to call job security security issue when security studies has been more naturally focused on war and peace and military conflicts? So are we diluted? Are we diluting security studies to the point of meaninglessness?  That's the same, I guess, argument with critical infrastructure. | | |
|  |  | P20 |  | About other other things being added and the challenges that provides, I mean I think the challenge it provides is from a policy point of view, if you keep adding to what you conceive of as critical national infrastructure.  And you're giving then agencies the responsibility to manage that infrastructure and protect it and secure it. It becomes an ever expanding thing that they're responsible for. And we don't have the resources, the manpower or the regulatory policy or the laws to actually effectively do that. So if we're adding everything into the critical infrastructure bucket and calling everything critical infrastructure and then expecting people to deal with that in effective ways doesn't seem to me very achievable.  From a policy or resource point of view.  There's also concerns that I've heard about you dilute then what really is critical. So if you count everything, then the the term critical infrastructure protection becomes meaningless. I'm sure you've heard this stuff before as well.  So, you know, should we talk about election and democratic processes as critical national infrastructure? Maybe we should just keep it on the, you know, the more traditional transport, energy, nuclear, whatever side.  I'm on. I'm not advocating any particular kind of view, but I I get the point, the broadening the scope and the definition the category.  You know, could make.  You know, could make the court that call meaningless and and this is a similar debate about security as a concept in the post cold era. | | |
|  |  |
|  |  |
|  |  |
|  |  | P20 |  | Yeah, I've I've seen it. Definitely, as I mentioned before, as a broadening trend, there are increasingly increasingly things that are categorised as critical national infrastructure when they haven't been before. You know, I'd probably put cloud computing in the in the Internet service provision bucket as you were. Obviously it's part of integral part of what's offered by Internet service providers now and.  And I guess for a long time, the cloud security thing has been quite quite prominent. If we shift all our data to the cloud, does that make it safe or not? I've never been entirely convinced it does.  So yeah, look, I I think that that's.  You know that's a worrying trend and you know, not least because the amount of data that's now stored in the cloud provides these vast repositories, which can be exploited for, for AI and used to to teach AI. So we've got a sort of a conflict emerging about access to data.  And how data is managed, particularly the data that's stored in in the cloud, as it were, which again, most people seem to say whenever these conversations happen.  Obviously it's not a cloud, it's a. It's a big room with a load of servers in it. In the United States predominantly.  I worry about European dependency, particularly on American cloud service provision. This is a problem.  And so yeah, I mean, I'm sort of zeroing on on cloud because you've mentioned it, but I guess the question was more. | | |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 93 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | Right. Got it. So so, so the two sorts of data we're talking about then are data about inventions or things that are assets you know?  You know, competitive assets in terms of of of technology and things that are.  Presumably things that would allow people to be manipulated and as they say things about.  Personal, sensitive personal data. If on a large scale, yes.  That actually is can be regarded. Ah, so we have got another sort of critical infrastructure.  Yes, you know, if I've if I've got a Jean bank about, you know, describing describing several million UK citizens, I have something that is pretty critical because. Yeah. | | |
|  |  |
|  |  | P21 |  | And I think both during COVID, but then also in our ransomware incidents, we've seen that education and also particularly schools as also a measure of daycare like it's not just not just the teaching bed, but also the daycare, the family structures, the way society functions on a day-to-day basis.  That they are sort of critical.  Central to yeah to our societal structures.  Yeah, I think that that could be something the way an expansion of C and I would in what in my area, I think it would hopefully imply that more businesses, institutions, organisations would fall and then what bindings are the security standards and measures? | | |
|  |  |
|  |  | P21 |  | Education, I think. | | |
|  |  | P22 |  | Just the the funny story of 2/3 of the firms in the greater Paris area, as it were, signed up with Amazon Cloud and Amazon Cloud, said they had back up, but unfortunately both clouds were on the same piece of the ETF network and when that went down for 24 hours, 2/3 of the companies in Paris were out of action. | | |
|  |  | P22 |  | And so talking to the chief architect, I think is called at British Airways.  One of the big problems was finding a backup cloud for some of the places where he had to have data centres because obviously it's a wide worldwide network and it goes to some, you know, goes across the Middle East and so on and.  But they had built into all their thinking that would be a resilient cloud, so the applications assumed everything was going to keep working, so he couldn't. He wasn't, didn't have the budget to build into his applications, ways of checking if things were failing because the assumption was the cloud would keep working. | | |
|  |  |
|  |  | P22 |  | we drew a little picture at the beginning of our study saying, you know, here's a A Venn diagram also. This is the, this is the software.  In use in the UK, this is the software developed in the UK and so in improving, yeah.  Slightly overlapping but and so in terms of improving the productivity of the UK, keeping the cnir, yeah, it's, you know, it's not within our control.  Because you're buying, you're buying software that's on the open market. You have it or you have not. And cloud computing is in that category and. | | |
|  |  |
|  |  | P23 |  | Lot it's it's become a major concern.  I I also work for a law firm.  We represent only startups.  Or formal advice at the moment is not to accept investment at all from China.  It's too risky and it can essentially get you into trouble with federal regulators.  And there's nothing you can do if that the Cepheus process of its triggered.  There's nothing you can do it.  The issues pertaining to any data, not just things, but also any data that is sensitive, which is soon soon people are gonna figure out that all data are sensitive. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 94 of 316 |  |
|  | | | | | | |
|  |  | P23 |  | And so right now it's things like location.  Umm, but you know in the US we stopped the acquisition of Grinder which was a a kind of a a dating app if you will for people who just wanted to have sex.  And what the kind of behind the scenes there is that a huge number of servicemen, we're using it and the the.  So the US government stepped in and blocked the deal.  And so I don't think if if you were designing such an app, you would ever think that the government would show up and block right?  Umm, so the supply chain issues, I mean as you know here in the UK, the amount of pressure we put on your government to remove Huawei from your stack, we're doing that internationally and we're trading on that, the nations that umm are willing to remove while Wei and other Chinese from infrastructure from their telecommunications get other benefits or intelligence sharing and other types of favors.  I'm so it is a major preoccupation in the US right now.  Linked to Taiwan and you know, whatever happens and whether we can get a silicon factory going. | | |
|  |  |
|  |  |
|  |  | P23 |  | Yeah, this this is a fundamental problem.  We so in my when I teach critical infrastructure protection, the exercise I have is I ask the students to eliminate criminal critical infrastructures. | | |
|  |  | P23 |  | Supply chain criticality as being, you know, a major issue and and not handled very well in law and procurement either.  It did have you come across that one at all. | | |
|  |  | P23 |  | They're they're, in fact is a statutory definition.  I can send it to you if you email me afterwards, I could send it to you.  There's also policymakers have proposed some, but the president gets to in the US, the President gets to establish an area is a critical infrastructure.  So the definition can say X, but then the president can say I hereby declare so and so critical infrastructure. | | |
|  |  | P23 |  | We we look at the list and I say OK, the government doesn't have enough resources to realistically protect all these things, which would you eliminate and it produces a really interesting discussion of what is critical.  So I I this is absolutely a concern as I as I mentioned under the US rules, even shopping malls.  Can apply to be considered critical infrastructure which is which begins to bend the concept of what is really critical. | | |
|  |  |
|  |  | P24 |  | Yes. So it's the like daily tools that we use like Alexa for our life. Then there are like bigger like higher level AI applications and people were saying that for example in terms of GPT.  More students are relying on this tool for.  Doing the research assessments, like many academic things, but at some point this is.  There is this dilemma that.  People don't trust these tools as much, but at the same time they rely on them. So in general we.  At the beginning, I guess we were reluctant on trusting cyber tools and for example, before COVID, I didn't do any. | | |
|  |  |
|  |  | P24 |  | In the young generations, let's say, but I didn't trust it as much at the beginning and after COVID when it was the only option.  Will you explore that? And then you think, oh, no, I I don't want. I don't need to go back. But if it doesn't work.  You tend to forget how it worked before, so in general I I think that we forget how to do backup plans because we're very comfortable relying on a digital tools and maybe it's harder to cope with this disruptions now.  Because comfortable relying on.  This easygoing alternatives. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 95 of 316 |  |
|  | | | | | | |
|  |  | P24 |  | Well, I I like these examples.  Quite interesting how?  We all as a society are being more dependent on.  Many of these cyber things and.  I I recently had a discussion on this.  Oh, what artificial narrow intelligence.  Narrow intelligence. | | |
|  |  |
|  |  | P3 |  | So that that sort of notion of what is a critical infrastructure or you know critical service provider, you know it sort of shifts a little bit. | | |
|  |  | P3 |  | Yeah, cause yeah, if you if you have libraries that are part of your that are critical to your business continuity or your societally critical infrastructure that's provided by GitHub, then you, you know that's that's important, right. | | |
|  |  | P3 |  | You know the the huge issue you know basically like with supply chain you know a lot of it is around you know understanding your supply chain, who who, who are they, who are the you know you're critical suppliers you know, do you have a good set of communications to them in case you need them. | | |
|  |  | P3 |  | So it's not maybe critical in the sense of like the NIS directive or what the UK, you know called CNI. | | |
|  |  | P3 |  | And I and I guess this sort of the thing as well, that sort of really hot in this area is supply chain, right?  And so that the criticality of the supply chain is is sort of there.  And so the these critical infrastructure operators known, do they have an interface to critical infrastructure? | | |
|  |  | P3 |  | So if you go back to the kind of smart grid kind of area, you know, there's sort of, you know, you to use a horrible American expression like mom and pop type organizations with relevant, you know, you know, I'm obsessed with security, but with relatively low security maturity or whatever kind of having sort of quite relatively critical interfaces to just sort of critical infrastructure operators.  So yeah, I would say it's generally great and I think that's also evidenced a little bit.  So in Europe we have this NIST to directive.  I'm sure you're aware of and sort of in the first version of NIS.  I mean, this is maybe just a staging thing, but you know, they talked about operators of essential services and digital service providers, right? | | |
|  |  |
|  |  | P3 |  | Do you have the contract language in place where they're obliged to support you if something goes sideways, all those sorts of kinds of issues, so they kind of become essential to your business continuity.  And so I think people are just starting to wake up to this now as a sort of a bit of, you know, as a sort of significant issue.  And we're still very early. | | |
|  |  | P3 |  | Essential to the operation of if if these these sort of critical infrastructures that we have, and so, so just to give you a bit of an example like in the nuclear sector, the UK civil sector are now doing a supply chain mapping exercise sort of like OK, who are our suppliers and then sort of looking at well if there's these sets are support you know they set of suppliers that are providing to the UK civil nuclear sector, what's the overlapping set, right?  And then all of a sudden we've got the set of organizations that turn out to be critical to the UK civil nuclear sector, because if they disappear for whatever reason, uh, we're kind of a little bit in a bad shape because. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 96 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | But, but you know, I nevertheless sort of critical to the business continuity of the their, you know their customers, right, who happened to be CNI | | |
|  |  | P3 |  | If you start thinking about it in those terms, you sort of need to widen the net a little. | | |
|  |  | P3 |  | And and you know that's that's, you know for quick infrastructures, you know the supplier systems integrators, suppliers, you know the the sort of you know uh essential to any kind of like security response because you can't touch it to often you know use an operator you can't touch it touch these systems because you don't you know because of the contracts that you've got set up or whatever so you need them to be available to respond to to failures and incidents. | | |
|  |  | P4 |  | This development pipeline stuff we're talking about, it's the expectation is that's going to run on a cloud infrastructure, but it's caveated on the basis that Ohh MOD cloud infrastructure but cap it on the basis that it should work on isolating infrastructure too.  But that's probably nothing is really jumping out with me as as a particular concern about extra infrastructure as it were, because the infrastructure cause it, it's where usually quite mindful of.  Platforms and this sort of boundaries and stuff, and the implications of what happens if they get extended. | | |
|  |  |
|  |  | P6 |  | And now that also due to the Russia war, we experience that we were assuming that all these IT platforms are always available 24 hours a day, no interrupt.  They are robust, they are robust and resilient.  And we can do everything out of it. And so we got rid of any kind of stock in our system for everybody, private and business. There is no reserve. There is no alternative. We just build on it and run. And Russia showed them that unbelievable. So if we do not have our e-mail system.  Or we do not have our well miss teams, so we are not using, we cannot do our, we cannot do our. Your interview cannot do our business so.  We already lost what I was called to and we lost the other call we lost.  There is no reverse mechanism any longer. We cannot go back to the analogue world. This happened already, so it's no longer just a power plant and the energies of provisioning. It's also the normal private, call it private non critical, non safety critically IT infrastructure, the normal telecom networks became already critical because no business, no private life.  And I believe also no governmental broker is feasible. I mean we are changing to online texts mechanism, every passports, everything is online now. | | |
|  |  |
|  |  |
|  |  | P7 |  | But it might not share the sort of common physical and technical characteristics with with, with other sectors, so this you know the the kind of thing that I talked about before the interface between the physical and the digital world. It's something that's, you know, in cloud computing does not really exist.  Or, you know, you can. You can stretch it but, but. But what I mean is that, you know, it's not. It's not necessary that that you have in cloud computing industrial systems that are controlled by by, by the cloud, right.  Or or that the you know the businesses that you are referring to and because and that make them cloud computing a critical infrastructure are fully digital, right? | | |
|  |  |
|  |  | P7 |  | Would it make a difference if we call the cloud a critical infrastructure? I I don't think so. It might create a bit of confusion I suppose to people that that that will think why? Why is it but some? Yeah, but I don't. I don't see it as a problem. I haven't thought about it very well though. So there might. There might be corner cases that.  Can create problems, yeah. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 97 of 316 |  |
|  | | | | | | |
|  |  | P8 |  | In the short term, I don't think so. In the mid to long term it may be yes, I cannot put my finger on it, but in the shorter term I don't think, but it's my personal opinion because we don't see any evidence at the moment, but mid term long term yeah probably did everything else. Yeah might be might be might be again, I'm not saying we'll be it might be. | | |
|  |  | P8 |  | So one thing is more forms of infrastructure are becoming critical.  So cloud computing services and so on, is that likely to be an issue at all in rail? | | |
|  |  | P9 |  | I think the the the one that's in that space. OK, yes, the information model of the society is going to be part of the critical national infrastructure. I'm going to tie it back to my previous debate.  It's been a slow evolving social construct over many years, but it's been, you know, national culture is something which is, which has integrity.  Two things place that's at risk going forward. It means we have to start to think about it in the same vein as we do critical national infrastructure. So our national culture.  Is an asset.  And I will again, I'll go back to Howard Lasswell. In the 1950s writing about security and propaganda in the US.  And say now we finished World War Two, our country will go to the dogs. If we don't have an enemy outside because we are too dispersed. So we will define ourselves as Americans as being everything the communists are. | | |
|  |  |
|  |  | P9 |  | So this the bar was really, really high by the time I got to be involved in the conversations around the National Risk Register and national security risk assessment and so on, the bar was, if it puts a minister on the front page of a newspaper as CNI, it really it really was down at that kind of level. | | |
|  |  | P9 |  | And so I think that that's a piece of information infrastructure that's important.  And I know I say the other side of that coin is as our society gets more digitised and this is something that and I talk about in terms of the, you know, the Metaverse and the spatial Internet, where a digital twin of everyone and everything, bits move, atoms move with the speed of bits. And we're basically living in this mixed corporeal and digital world. That means that our society has a digital representation and a model.  Information model the taxonomy and ontology a set of standards. That is a piece of critical national infrastructure which needs to be protected because of that information model fails. It'll have. It'll have real world consequences.  Again, it's it's somewhat less tangible than saying do you mean like the banking Ledger in the Bank of England? OK. Yeah, yeah, that too. But really, it's all of those sorts of things. So yeah, I'll put those two. I'll put. I'll put that that down as a marker and say for those two reasons, the information model of the country itself is a piece of national infrastructure. Also say then thinking about.  The economy and finance, so many of the services and systems and economic mechanisms that we use today are now running on a data infrastructure that could fail every. So the network and everything else, their information model matters. We've got interesting conversation with somebody about Central bank, digital currencies and whether they need to be secure against quantum crypt attacks. And the challenge of course there is in a cryptocurrency or processing time is your transaction time. So you don't really want it to be very secure because that costs a lot of compute. | | |
|  |  |
|  |  |
|  |  |
|  |  | P9 |  | So we do, we want to be careful. We're we're we're we're extending this for the right reasons. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 98 of 316 |  |
|  | | | | | | |
|  |  | P9 |  | But we need to start that conversation from the point of going our national vision and culture is a it's a national asset in its own right, and we need to recognise that there are people who wish it I'll and wish to subvert it to certain outcomes and not all of them have a legitimate stake in that. | | |
|  |  | P9 |  | And take practical steps to make that true.  And it's interesting to look at American Society since the end of the Cold War.  And wonder if he wasn't right, but the but the sense what's really important there is the sense that that national identity and vision of what it means to be a nation is a thing that needs preserving. Now they've never been able to evolve as quickly as they do today.  And they've never been under attack from multiple interest parties as they are to date. Because of that information domain. So if I'm allowed to put take some of my existential rant and put it on the table, I think our national narrative is a piece of CNI that needs to be protected. And the dividing line between protecting and nurturing it and attacking it is two sides of the same coin.  The reason I say. | | |
|  |  |
|  |  | P9 |  | Supreme | | |
|  |  | P9 |  | I mean, you talk about the fact that the compute layer is now CNI, when it wasn't before and and a bizarre range of online services.  There is a there's a. There's a risk pattern emerging to come back to this adjacent possible idea, and the fact that innovation is connecting things together. People are building services on the back of really, really flaky previous services and then at some point it suddenly becomes desperately important and you realise that underneath it, you know, there's a fantastic XKCD cartoon where we say another one, lots of. Yeah, that's it. Yeah, that is it. That is it. | | |
|  |  |
|  | | | | | | |
| **Funding** |  | | | | | |
|
|  |  | P15 |  | Better having a better understanding of how previous risks have manifested themselves and and learning what other people have already learnt. We do a lot of relearning what we already somebody already knew, but then they left the organisation. So there's a lot of sort of epistemic like knowledge loss about things.  And therefore like if there's a big churn of people who are constantly circulating around, then that doesn't necessarily stay within one organisation and therefore their organisational ability to respond as it's gone because that's it's with Bob and he's been here for 20 years.  So again, I don't think I've answered your question very well.  Can you remind me what it is again please? | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 99 of 316 |  |
|  | | | | | | |
|  |  | P15 |  | What keeps me up at night?  But also so then again.  If we're being really honest, it's what keeps me up at night. Is there aren't enough emergency planners doing things because there's not enough funding? Certainly.  I would say not necessarily in commercial entities because I don't know that so well, but the.  I would say it's a greater a sense of how.  How different organisations that are multi agency perspective are able to operate together.  So any kind of major instant response or major emergency or disaster response is never going to be just a single agency working on their own. | | |
|  |  |
|  |  | P15 |  | And I think my kind of fears are we might have been in a good position X number of years ago.  But things are being like eroded quite a lot, and therefore people know stuff should be being done, but particularly in the health services and local authorities and and police and stuff, there aren't enough people doing it, even though they know and the people who are working there are are working under very different pressures. So I think it's probably those.  Like resourcing and funding kind of issues because they underpin literally everything that you're doing. It's all well and good saying I'm, I know I'm really worried about the situation in Ukraine, the impact that's having on fuel, the fact that we're like quite likely to have.  Major fuel issues if we have significant bounce of cold weather, we're going to run out of fuel and and we'll have issues around that. But like there.  They're sort of risk specific. I think I'm probably more worried about the more general context of.  How everybody works together in in a bigger sense, political direction in major incidents.  Which can be erratic at best.  And and their engagement in emergency response in advance of the incident. | | |
|  |  |
|  |  |
|  |  | P15 |  | And sort of senior leadership engagement in those plans. So one of my greatest frustrations I think, has been I've spent a number of years working on lots of things. And then the the incident itself has happened and then the plans that I've helped people develop just don't get put into action, which is very deflating. And I I am not the only person who has said this.  Not not to the same extent. | | |
|  |  | P15 |  | And then it tended to then sort of move to local authorities and now all working in a much more sort of multi agency perspective in terms of having much stronger local resilience forums, which are sort of multi agency by nature rather than people just sort of sitting together. So I think there are but within that at the same time it's it's had to be more smart because there's hardly any resources for.  What's going on? So where teams might have had, I don't know. Hypothetically, there might have been a team of 10 in 2000 and eight 2011 on the run up to the Olympics in London. Teams were very well resourced. And then after that it's just been steadily eroded. And therefore, you're working with much smaller numbers of people.  And I think that that is not a dissimilar situation from two other count one and two responders where people are double hatting.  I don't know how you solve that necessarily, other than magically coming up with some more funding that wouldn't otherwise go to the NHS for day-to-day service provision and schools and education and all the other things that we need money for.  So I think there has to be a way like if there can be a way that technology can.  Enable the limited human resources to be more effective in what they're doing, so they're not spending. They're not all spending a day looking at this risk and doing the same thinking they can get that thinking from because somebody else has done it and they shared it with them or whatever it is.  If technology can enable smaller number of resources because unlikely, we're going to magically just get loads more.  Then that would be useful also better understanding. | | |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 100 of 316 |  |
|  | | | | | | |
|  |  | P4 |  | That hardware is going to become obsolete, usually with space missions.  Now it's all done on on an ad hoc basis, or at least it was in my time because Mars Express, you know, it's gonna be 3 year mission now.  It always gets extended because there's a little bit more.  There's a little bit more sort of battery.  We found a little bit more funding, but it's all it's always done on, on the on all this premise on the basis that we might just lose contact and everything will basically finish, but it's certainly with the other project I'm involved with at the moment with this mod development pipeline, we're gonna one of the requirements we've actually put in is this is gonna have to run for several decades.  And how are you going to make sure that that knowledge is sustained over that period? | | |
|  |  |
|  | | | | | | |
| **Geopolitical Fragmentation** |  | | | | | |
|
|  |  | P12 |  | I think in the next 5 to 10 years, we'll probably see just this broader trend toward what I what, what my post OP advisor and what I now kind of also have taken on to this idea of blocks. So you know the US and its immediate allies in North America kind of represents one block, whether the EU will be a part of that block remains to be seen, right?  And then China and it's Belton Rd allies are another block and and, you know, potentially India is another block and then there are all these non allied countries non aligned countries. We'll see what they do and probably different things for each of them. And I and I think that in the next 5 to 10 years what we'll probably see is like a confluence of standards supply chains and technical infrastructure software protocols it all kind of dissolving into or or fragmenting into these blocks.  And you know, in a happy ending, these blocks are more porous between one another in a less happy ending. They're not so porous between one another, but I think that the world of, you know, we all have, you know, this one kind of set of Internet standards that is presumed to be canonical. Unfortunately, maybe somewhat not so long lived on the five to 10 year time scale. And I think in that five to 10 years we'll start to see, OK you know we don't actually all agree on this RFC. We don't actually all agree on this W3C spec.  And start to see that fragment and and you know I'll note here also this isn't all just about war and conflict. | | |
|  |  |
|  |  |
|  |  | P12 |  | Also, economic interests here, and surely you know meta, has an interest in kind of not listening to the West 3C. Sometimes Google has taken this route where it is the West 3C that's a big investment that it made in in stainless bodies, and then it has made that investment. And I think when you look at like, you know, their horizons and all their metaverse stuff, what they're saying is, you know, forget this W3C. The web is old. We're doing our own thing. And I do think we can expect to see more of that. That has nothing to do with more conflict about. Well, not nothing. But it isn't intrinsically about war and conflict.  It really is about, you know, commercial interest, but I think that these things are coalescing to produce that sort of block by block fragmentation that that's kind of mostly what I expect in the next 5 to 10 years. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 101 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Graceful Degradation** |  | | | | | |
|
|  |  | P11 |  | So you end up with systems that are much more.  Designed to be graceful in their degradation | | |
|  |  | P5 |  | And I say that because we're kind of going through a nuclear renaissance right now with the old big reactors to the smaller reactors.  It's all new type of design.  They talk about the passively safe properties of these, where there's no matter what, it's not gonna go and melt fuel or anything. | | |
|  | | | | | | |
| **Huge impact to CNI failures** |  | | | | | |
|
|  |  | P11 |  | At an engineering level is yeah, the Black start challenge. A black start. Let's say you are.  I tell you what, let's let's use the the example of the power plant in Ukraine, where the Russians have, you know, surrounded it and occupied it. You remember the discussion is that they need an external power source.  They need to be connected to the grid and you know your average person on the street will go, oh, I don't. They just generate their own power. Well, the problem actually arises that if you turn everything off.  It isn't a question of plugging in a 9 Volt battery and then suddenly you can bring it all back to life.  And if your grid goes down, it's actually quite hard to bring the grid back up and an example of that happened in the United States, where there's a domino catastrophic domino failure of the grid or some years ago now.  And actually that led to a lot of observations about the kind of control dynamics that I was talking about earlier.  It's actually quite difficult to island. It is quite difficult to isolate it and to stop the consequences propagating. | | |
|  |  |
|  |  |
|  |  | P11 |  | Even assuming you've just got a coal-fired furnace and you, you know you've got steam ready to go, it's actually quite difficult to bring the grid back up. So the whole idea that if you can cause if you can destabilise to some degree, you can actually just you can actually take down the energy system that I think is one of the concerns. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 102 of 316 |  |
|  | | | | | | |
|  |  | P14 |  | Sewage systems fail.  Transport systems collapse, health systems collapse. | | |
|  |  | P14 |  | Power across the globe.  Internet across the globe could be seriously affected, but if it was actually only in the UK, take out enough of the.  Electronic the other sort of net, the network, the electronics power, net grid network.  I think it might be at the moment 18 months lead time before Germany would provide you with a new piece of kit. Take out a lot of those and you have no electronics, no communications.  Profound failure on society, to the point where people might almost be drawing weapons and fighting one another. You know there are some very, very serious.  Because supply chains go down, communications goes down.  Government can't communicate with the people to provide any level of assurance or reassurance.  Water supply runs out. | | |
|  |  |
|  |  | P19 |  | And when I kind of horrific attack.  And for for example, there have been attacks on on power stations, on telecommunications facilities in the US have been bombed.  But I was asked to comment on on the likely recovery time for one of these couple of years ago that these are very difficult to to stop.  Of course, yes, I yes.  But but you have to be one of these incidents happens that the most important thing, I suppose, is that the customers who depend on the on the service and it might not just be.  Yeah, I said.  It might be hospitals and indeed other critical yeah systems.  So it's very important to make sure that these kind of systems are protected and the that things don't don't get very bad very quickly. | | |
|  |  |
|  |  | P20 |  | I guess probably I'd say ransomware appears to be the the big problem in terms of its ability to shut down bits of critical national infrastructure. I was just reading a report yesterday about an attack against the health sector. Again a Children's Hospital.  Being basically blackmailed for millions of dollars to to get their data operational or get their data back.  So I think.  You know, I'd say ransomware is a particular problem. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 103 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | it can be an existential threat, that sort of business interruption. You can't manufacture, you can't produce, and so on. And as a result, you might have additional cost, loss of income, reputational harm and so on. But I think ransomware causes so many other kinds of harm that are sort of overlooked in that context. And that includes if there's ransomware attacks against critical national infrastructure, for example, the psychological harm that people face as a result of ransomware attacks. If your staff member working on this, it's particularly grave for it teams because they often feel personally responsible.  Work themselves into a burnout and then if you have an IT team that's on burnout, you know that they make worse decisions for your cybersecurity as a result as well.  At the same time, when critical national infrastructure is.  Implicated and we talk about it a little bit. Education doesn't fall into this, but let's assume a hospital or perhaps government structures that pay our benefits.  There you see a particularly harsh impact on those that are already vulnerable, which I think has societal implications as well. So you might think about the patient waiting for surgery. You might think about the benefit recipient of a local council.  You might think of those who are dependent on council housing or something like that.  And they fear particular consequences as a result of ransomware attack. If you're a multinational corporation, you have the the skills and the capability and the experience dealing with a crisis. If you're a local school, you don't. If you you don't, you just don't know what to do and you're kind of crisis is a different crisis that you're used to. You're used to being someone getting lost on a class trip or something like that, but you're not used to handling the cybersecurity incident and.  We found in our research that that kind of attack in terms of societal implications means that those that are already vulnerable feel more of their harm or are affected disproportionately. | | |
|  |  |
|  |  |
|  |  |
|  |  | P21 |  | something that would keep me up at night is a coordinated ransomware attack against water systems. Water systems are relatively distributed, but you could imagine a scenario where. | | |
|  |  | P21 |  | Maybe several attacks at the same time, or quite quite impactful. | | |
|  |  | P3 |  | I mean, yeah, if I if I was to talk about kind of the nuclear, you know, the major of course that's the thing that we're most concerned about is nuclear safety, right?  So any so any kind of cyber, cyber induced you know?  Nuclear safety related incidents or release of material. | | |
|  |  | P3 |  | Perhaps then, of course, this nuclear security right?  So theft of the material right is it is a huge topic. | | |
|  |  | P5 |  | I mean that may not be as dramatic or anything or maybe it wouldn't shut the whole industry down, but it's certainly would put everyone on pause.  It would cost a lot of money for people to say, Oh my gosh, these guys got into this nuclear plant in France.  We better check all of our nuclear unit solving our country to make sure we're not susceptible to the same thing.  So it's going to cost some money for sure. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 104 of 316 |  |
|  | | | | | | |
|  |  | P5 |  | Yeah, using the technology against itself, pretty much, you know, towards that sabotage.  That's immaterial.  Whatever their goals are in life, or it could even be something that, you know, they could do anything successful from a cyber attack and that could shut down the nuclear industry for a year. | | |
|  |  | P5 |  | Yeah, not probably the sort of mass disaster that, that, that people are looking for, but a tremendous it would be.  It is a tremendous commercial worry that something like that might happen, yeah. | | |
|  |  | P7 |  | Well, if if this was if this was a nuclear explosion would be would be much worse, I suppose. But but. But I think I think you know it's.  The interface between between it and OT right? Generic ICT with operational technology is what, what what creates this this challenges.  So yeah, I mean I I I don't want to say specific examples about nuclear because nuclear, you know, is an industry that is very sensitive to to even to rumours. | | |
|  |  | P7 |  | It has to be nuclear.  Any any industrial system that interfaces physical processes with digital processes?  You know, and if if you if you interfere with the physical process, all sorts of things can can start happening.  You know, I'm sure I'm sure you've seen the videos from the from the attack on the steel manufacturing plant in Iran last last summer, things started exploding. | | |
|  |  | P8 |  | Please take a note of it is the it's depending on the environment, right? If I press on the wrong button because someone made me in McDonald's, I buy 2 happy meals instead of one. I lose Â£5. OK, I lose Â£5.  If I press on the wrong button in a nuclear reactor because someone made me so that's why. Please take into consideration of the environment. So the consequence of what happened is depends on who is the user and my safety critical operator or am IA mother try to buy to help me. The consequences depending on the context, the context, environment, the consequence of can be anything from therefore injury.  You know, if I was in a nuclear reactor, I place on the wrong button, everyone dies.  That can happen. We don't know if it didn't happen.  Two reputation loss, a lot of reputation loss tonight because if you, the other consequences, you know the Council or the police and you give all the data away, I trusted you with my data and you gave it away to everyone. Reputation lost. There you go.  Reputation is a bigger loss, in my view than actually sometimes because you know the reputation means sometimes. Look, if there's a train accident because it travels fully, city is the driver's fault.  Maybe the people think, baby, relax them to take the train for a year, a month or two. But then if they say that the trains or the planes are susceptible to cyber attack always I will never take them. I will never in my entire life take them. So therefore reputation loss can be worse in the sense which means financial loss. Obviously a lot of the financial loss that comes with it and I think it was in the paper as well. So we talked about financial loss.  We talked about all the data loss and everything. | | |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 105 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Human in Loop** |  | | | | | |
|
|  |  | P19 |  | been in a few telecoms control rooms and the people there use lots and lots of new tools.  They they, they observed in measure the the I think they don't yet close automatic control loops about.  Using these tools, at least the until the test Rd tested them, which is difficult to do.  And so they keep a.  You mean they keep it?  A human in the loop, but the the Human envelopes? | | |
|  |  |
|  |  | P23 |  | I think we're gonna need a lot of work to manage the.  Ohh, the disasters that we're going to experience, for better or worse. | | |
|  |  | P23 |  | I wonder if it's.  If we're gonna have a, we're essentially gonna have to have an AI bureaucracy to deal with the things that are going to happen. | | |
|  |  | P23 |  | is I'm the high reliability organizations, they require big bureaucracies and and so people say AI is gonna kill all the jobs I'm making to wonder if AI is going to require the ultimate kind of management bureaucracy. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 106 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Hydrogen for Power Supply** |  | | | | | |
|
|  |  | P9 |  | within the Christian life, Christian life, infrastructure space, what we're seeing now is we're going to move from methane gas pumping through networks. Those asset base is about Â£14 billion worth of underground asset there. That's going to get completely useless. So there's going to be a lot of work put into trying to reuse it or something. Is it what you just put hydrogen down there, OK, hydrogen network, you can't pack for pressure carries per mass. It carries 1/3 less the amount of energy it flows that very, very much faster and it leads a lot more easily. So you could upgrade your system, the maintenance schedules are higher.  And you've to reconfigure the feed in and feed out of the system and run and run it to storage, because you can no longer use the network for storage, you're going to have to do that every 30 minutes instead of every 24 hours. Now the complexity of managing that system and then interfacing it with the different contracts because people only want to pay for the kind of gas that they want put into it, that complexity. Now you add electricity, which we've simplified the market enormously by just doing marginal pricing rather than pricing by type, which is going to be coming.  That combined with water.  We're doing hydrogen. The hydrogen economy predicted for the UK will mean we need about three times as much clean water as we currently have in the entire country, so the whole water network is going to get boosted 3% of our energy bill already goes on running water system in the UK, so you can expect that to go up and then you've got the waste, both in terms of waste energy and in terms of the waste products of that, which will then run through a series of efferent networks out for sequestration through the carbon being pumped, that the homeostasis of the pumping lifeblood.  Of a of a of a of a geographic region is going to get much more complex in order to keep it within the bounds of what we can put within the energy envelope of the planet.  I think that's going to be a really interesting problem and I think that is going to happen within the next 10 to 15 years.  15 years we've got no chance of making our temperature targets, yeah. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  | | | | | | |
| **Improved Logistics** |  | | | | | |
|
|  |  | P8 |  | Can be designed and integrated the system to human nature I am expecting.  Is to get better because we are pushing for it.  I'm hoping I don't know this my English hoping and expecting are different things I am envisaging it's it. I envisage this to get better because there's more and more progress done in this area right now, so I'm quite positive I'm quite hopeful about this to be honest, because we are now a better systems. We now have a better integrated systems. If we get better, I'm hoping again.  Hop slash XP I hope them to get better. I expect them to get better. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 107 of 316 |  |
|  | | | | | | |
|  |  | P8 |  | It could happen, although this might be looking into human factors because you know the humans will not change that fast. We will always hear people who are a bit older. We will always hear people with disabilities. We will always have people who don't like technology, so I assume they will not be fully automated, but some kind of game changes. They could be that around the stations from the passengers point of view, I could imagine that and also the touch points what we call is RAD.  They say the passengers leave a pass or a taxi or the tram, and then they travel to the station. There could be more.  So this process could be more streamlined. I think the process of door to door travel door to door, I mean from the house to wherever you've been to get to, I think there's a lot of game changes in between of those interfaces. So not in one place, not in a control of another, not on a train, not on a station. Not a lot but a lot of that thing changes will happen in between which doesn't look like.  A real network, but I think from the door to door journey point of is a railway network. | | |
|  |  |
|  |  |
|  | | | | | | |
| **Improved Training in Software Contracts** |  | | | | | |
|
|  |  | P22 |  | You're dependent on boarding component. You get, you get no support from procurement, you get landed with impossible contracts, like if it breaks, it's your fault, not the suppliers fault. | | |
|  |  | P22 |  | I would hate to be a CIO these days. I think it's a really awful position to be in. | | |
|  |  | P22 |  | Procurement doesn't have the capability of looking at software contracts. | | |
|  |  | P22 |  | all part of more people being able to cope with it rather than saying purchasing contracts for it. It it is a big part of the purchasing world, so more people should be aware of it contracts rather than regarding just special, I think | | |
|  |  | P22 |  | so it's it's computer literate purchasing people not not.  Not purchasing literate, IT's people that we want, yes. Yeah. | | |
|  |  | P22 |  | There is a big issue which is and it may happen just with a generation change that you know if you're a 2 year old that sort of started off pressing T at the age of 2.  And, you know, found that things happen. Maybe you just are more it illiterate by the time you get to 30 and are able to go once an IT contract. Yeah. I'm a contract manager. It's an IT contract. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 108 of 316 |  |
|  | | | | | | |
|  |  | P22 |  | So who's going to look at an it guys aren't good at reading contract?  Why should I be yourself? So it's a big job. And so some of the procurement people we talked to on the working groups were really concerned about this. But you know, again they were trying to find somebody who was aware enough of the problem to start talking about it. | | |
|  |  | P3 |  | Do you have the contract language in place where they're obliged to support you if something goes sideways, all those sorts of kinds of issues, so they kind of become essential to your business continuity.  And so I think people are just starting to wake up to this now as a sort of a bit of, you know, as a sort of significant issue.  And we're still very early. | | |
|  |  | P3 |  | You know the the huge issue you know basically like with supply chain you know a lot of it is around you know understanding your supply chain, who who, who are they, who are the you know you're critical suppliers you know, do you have a good set of communications to them in case you need them. | | |
|  | | | | | | |
| **Incident Planning Training and Exercises** |  | | | | | |
|
|  |  | P12 |  | I think the financial system's actually really robust. I I I did. So I have in this research spoken people inside the financial system, which is really hard to do because they really don't want to talk to you and they don't want to tell you also how anything works. But I'm actually really convinced like they're table topping. What if the Internet goes down in a way | | |
|  |  | P16 |  | Understanding making that complexibility more visible and less surprising, I think and is is probably one of the answers I'd like to put forward and the way to do it to do it probably would be by developing more simulation and stress testing capacities.  For this complexity and I, I think that the UK has been very has been very.  Has been forging ahead, especially I I know the financial sector better so, but using the the you know the.  What's the name of that exercise? The red teaming exercises so that the Crest.  Type of approach where. | | |
|  |  |
|  |  | P16 |  | The regulators are testing independently the business and the reliability of the of the systems of its regulates and helping them identify weaknesses and and and incentivize them to to fix them. So stress testing and simulating and.  Learning to operate under very, very hostile.  Circumstances by default. | | |
|  |  | P21 |  | Capabilities to respond to something, perhaps. | | |
|  |  | P21 |  | I mean the UK has capable, it's called assert, a cyber emergency response teams, but the NCSE is good, but they.  There's also limits to how much they can do so if it's a coordinated effort that I'll matches. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 109 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Incident Response Different for OT** |  | | | | | |
|
|  |  | P17 |  | Because like I say, you got different protocols, you need different skill sets to understand them. If you're dealing with OT, it's very engineering led. If you've got it, it's not very engineering at all. You know, it's very traditional it computing stuff. So you've got to complement that and that's going to be a real tricky thing that I don't think is going to be solved anytime soon. | | |
|  |  | P17 |  | So it's not like you can just let some SoC analysts kind of go. Yeah, cool. Let me disconnect that. And there'll be certain things that can do, but you can't just do things hastily. So I think, you know, the instant response approaches are very different in those things. So that's why I'm saying you can't just have one box or one system that just consumes it, or as much as we'd like it to, because that makes life simple and logistically. And if if cost efficiency and whatnot. So as a as a follow up to that, then you're going to have different systems looking after.  Those three different domains, right? So the questions then are asking them, well, actually, if I've got my IET connected to my OT to provide an overall time sensor in and stuff.  How do I correlate a threat that's happening on my IoT that's that's also affecting my OT? Like, how do you correlate? You've got two different systems consuming, you know, two different datasets and there might be the same attack vector, but it started on that domain to that domain. So this this correlation between those two systems. And I think that's going to be quite difficult to do. So a lot of what we were looking into recently was like how do you look at different data sets for monitoring and how does that influence, you know, the future Sock effectively? | | |
|  |  |
|  |  |
|  |  | P17 |  | So for example, if you've got like some cloud infrastructure and you detect something that's malicious and you look into it and you, it turns out it really is malicious, then you can blow it, right? I'm going to shut down my systems. You know, I'm going to block my main gateway, which all our customers use. So we might have a down, an outage on whatever your service is. Basically. You know, if it's a payment gateway, for example, we're going to put it down for a few minutes so we can isolate it, do some instant response, some digital forensics, find out and isolate, remove and then follow up with some investigations. And you do almost do that immediately by your playbook.  If you're got a set of, you know network switches controlled in Plcs which are connected to workstations that control nuclear fuel rods into a reactor. You're not going to sit there and be like, right. Isolate everything, stop the PL Cs you know, unless obviously it's going to cause you know an over reaction of some sort. You'll obviously want to stop that, but yeah, those those kind of things, an instant response is is completely different because.  The rationale about making a decision has a wider stakeholder group that needs to sort of assess the safety impact of that decision. | | |
|  |  |
|  |  |
|  |  | P17 |  | And IoT because they all have different sets of protocols, different constrictions.  You know different implications, like the instant response is massively different in OT as it is for for it for example. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 110 of 316 |  |
|  | | | | | | |
|  |  | P7 |  | What is normal, you know a another consequence of of lack of connectivity is is, is is low visibility. In this environments we don't really know. You know, how do you even run, you know TCP dump in an environment like this to actually know what's happened.  So one thing one thing is is is AI. So when we have non obvious signatures low, low intensity dormant software potentially, how do we profile this? How do we profile the normal behaviour of these environments? | | |
|  |  |
|  | | | | | | |
| **Incorrect AI Response to Attacks** |  | | | | | |
|
|  |  | P15 |  | And therefore there are opportunities for things like that absolutely to be either intentionally or unintentionally.  Suede by AI doing that thinking for us.  So you you could potentially think a place is safe and choose that for where you want to put your all of your resources. And it turns out I know it's underwater or or it's in a in an in an area which could easily be that threat from whatever the risk is. | | |
|  |  | P24 |  | Like transfer these accountability to the tool, which is not actually accountable for that.  For trying to optimise things, but at the end of the day.  A human perspective and a assessment is always required. | | |
|  |  | P24 |  | And we we were talking about this in terms of a critical infrastructure that.  We had digital tools. We should.  Give all the responsibility to them to monitor the operation of a telecoms network or the.  Health of a rich if there's the money turns. If there's a sensors in it doesn't say anything is going wrong, then why should I send someone to do the visual assessment? It's not required. I will have extra cost. Maybe if I do that.  And then the issue is trying to. | | |
|  |  |
|  |  | P24 |  | You tend to forget how it worked before, so in general I I think that we forget how to do backup plans because we're very comfortable relying on a digital tools and maybe it's harder to cope with this disruptions now.  Because comfortable relying on.  This easygoing alternatives. | | |
|  |  | P6 |  | this problem even goes further when we come to the to when we try to prevent our critical ITOT infrastructure and we are applying AI for anomaly detection, I think which is a good illusion and we should go for it and researchers and they're working on it. So there are. | | |
|  |  | P6 |  | But of course, as soon as you're building it, you indent the system is identifying something. That's the starting point. That's again talk about complexity. It's a starting point because the system doesn't know, and you you as user of operate of the system, do not know. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 111 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | Is it now a failure in the system, or was the external attack you're you never know, so you get much more information you need. Again, more powerful IT systems which are sorting out this information that at the end you come to a kind of decision mode. So just applying AI is a very cool idea as a sensor, but it's not yet the solution. Solving all the problems we have to build on it and to build much more powerful system.  As we said at the beginning to master it.  And this question, accident or failure and remote attack will always be there. We have to find means in there, of course.  I got you. I got you. | | |
|  |  |
|  | | | | | | |
| **Increased Automation** |  | | | | | |
|
|  |  | P5 |  | And then the last one is just really quick before I get it in before I lose it is autonomous operation and that's where maybe the AIML type technologies will come into inform the operator. | | |
|  |  | P8 |  | Two in terms of the driver.  This the European traffic, you know the the management system again in the paper it is a full name of it. It is called like an ARTMS. So this is simply do you know the signals used to be like an out there sometimes and the job used to just look or is it red or is it they put you ugly now they are on the incap. So I think there might be more changes in there I have to be very careful what I'm saying. So at the moment I'm assuming even there's more automation if there'll be more automation.  The humans will still take a part.  Where we'll do more monitoring.  Although we know in other countries, they say, you know, in other places like in Dubai and so on, the fully automated systems are there, so they could be in 15 years time potentially. Again, I'm just in potential. I'm being careful here 1015 years time they could get more and more automated. So they'll look pretty much like an automated trains. I don't expect to see fully automated systems and controls because I think there should be some sort of monitoring should always be there. | | |
|  |  |
|  |  |
|  | | | | | | |
| **Increased dependency on tech** |  | | | | | |
|
|  |  | P10 |  | So, alright, so so this is a thing to look out for is where the the software or the the availability of these systems becomes such that you don't have the resilience of the old systems anymore. And that's a more general problem, isn't it that? | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 112 of 316 |  |
|  | | | | | | |
|  |  | P10 |  | over the reliance on technology, yeah, just just kind of erodes that kind of physical backup. So when I can't get you know deliveries whatever is actually I don't have the shops to go to anymore, they're not there and the supply chain that's bringing in you know various of these can't get through you know whatever can't get through put passport control and and can't get past you know various get those are the sorts of things we just don't have those resilience.  Anymore, yeah. | | |
|  |  |
|  |  | P10 |  | what if there's, you know, the all the job centres go down or or something, you know it's it's it's it'll. It'll just a glitch in the system and people don't get paid I think | | |
|  |  | P10 |  | . But there's there's again this is sort of database, there's evidence just that people.  Kind of trust in their organisational.  Sort of protections. You know, they might not trust at home, but on the work. I think if they work for government or work in, you know, a a critical.  Part of of of the Society or the financial sector or health or whatever, and so if they get a dodgy e-mail, they'll fall. They won't open at home and they won't open up on their phone because it looks, you know, they've used their intelligence. So they'll forward it to work and they'll open it at work because they believe, you know, that everything will protect them there and that that there's there's, you know, we know that people do this. And if that is kind of terrifying and that's the sort of someone who who thinks they're, you know, doing the right thing and and sort of almost trusting in the systems that we've said are in place.  And and therefore, you know sort of that that sort of cascading effect. | | |
|  |  |
|  |  | P13 |  | So there have been incidents where.  NHS systems have been attacked and, for example, medical record systems have been subject to ransomware. And while it's inconvenient, I mean.  Somehow the system keeps managing to work.  Reversing to older technologies.  So there is that. But I mean I suppose.  Increasing reliance on those kinds of technologies makes us more vulnerable to critical incidents involving them. | | |
|  |  |
|  |  | P13 |  | If you think about the relationship between patients and healthcare professionals, it's obviously one built on trust.  I don't think I see that being maintained.  Though of course I painted a picture earlier of increasing.  Let's call it algorithmic healthcare for want to the better word. And so your scenarios would fit with that. So there is potential that that could happen every we move in that direction.  I mean it. It's also possible that you see increasing sources of the misinformation.  And you see this, I think already not, not particularly motivated by AI, but it's the same kind of thing in terms of vaccine hesitancy.  Where actually | | |
|  |  |
|  |  | P13 |  | For example.  This could all go horribly wrong if, for example, you create a large network of data and then some unfriendly state act takes control over S and either steals it or does some kind of ransomware attack.  Then that would allow horribly wrong. | | |
|  |  | P6 |  | We cannot go back to the analogue world. This happened already, so it's no longer just a power plant and the energies of provisioning. It's also the normal private, call it private non critical, non safety critically IT infrastructure, the normal telecom networks became already critical because no business, no private life.  And I believe also no governmental broker is feasible. I mean we are changing to online texts mechanism, every passports, everything is online now. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 113 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | If the online platform is not working, we even cannot go to an office and say I need a new passport there. No money sent me electronically. The filled out form where we don't have it. So this happened already nearly worldwide and I believe we are not yet prepared, but that's my main nutshell. | | |
|  | | | | | | |
| **Increased Gopolitical Risk** |  | | | | | |
|
|  |  | P10 |  | You know, to, to, to you know, to to a dangerous time. I mean, I think it's we've always been living in dangerous time. Right. But I think you know that it's not as safe. It's not. The world is not a safe place for the geopolitics. Engaging, engaging here. Not not.  Not just focusing on the geopolitics, but, but you know they they obviously kind of setting setting the scene here. But I think you know some some real direction, some some.  You know, there is so many different agencies in in the UK in particular leading on this and then globally it becomes even more, you know, even messier. | | |
|  |  |
|  |  | P20 |  | a lot of this is again from my own point of view against the worsening geopolitical backdrop in which if there is a war in Taiwan, then critical infrastructure, cyberattacks against critical infrastructure might well play a significant part, whether it's Taiwan attacking Chinese critical infrastructure through cyber or Chinese, China doing, you know a preemptive preemptive attacks against.  Taiwan's telecommunications systems or its transport. | | |
|  |  | P20 |  | that's played out to some extent in Ukraine as well with attacks on Ukrainian energy grids historically for for political strategic gain by Russia. So I think as well as those sort of technical trends, behavioural trends.  You know all this is probably being worsened, accentuated by the the changing geopolitical environment. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 114 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Increased Use of Radio** |  | | | | | |
|
|  |  | P17 |  | I come back to that concrete sensor or if you've got like a real time set of sensors that are that are feeding, you know using wireless technologies to to feed an edge system.  You know, if you're able to intercept those signals, if it's using like a Zigbee or Bluetooth or an infrared even or an RF signal or some sort.  You know there's well, I mean you can you can buy one of these for like a couple Â£150. You know these flippers.  Which have just banned in Canada and you can start playing and interacting with them. So I think, yeah, there's definitely going to be a concern between how how complexity those signals are and then versus are they malicious. And I think the other concern I have which I'm not sure is probably quite relevant to this particular question is.  At the moment we do, but I've not asked personally, but as a society, should I say is very good at doing monitoring of enterprise IT systems and there is there has been for a while and it's going to grow a bit more in the OT sector.  It will be in the IO T sector as well. That will kind of follow up after OT, maybe it will overtake it at some point. What's interesting is where you've got a mix of both ITOT and IoT as part of your system.  And each of those sort of systems. So it's like free domains, if you call it that, they're all going to have the range sort of monitoring solutions the the, I mean Microsoft are trying to do it and a few other companies are trying to do it, but it wasn't just A1 box and you feed it all, you know it. | | |
|  |  |
|  |  |
|  |  |
|  |  | P5 |  | However, there is so much pressure being put on them, not only from vendors wanting to sell their products, but from the efficiencies that these new products are advertising, especially when it comes into outage control maintenance or they can walk around with a tablet, you know wirelessly and do their procedures and do their maintenance and just different walk around things that they do in the facilities that are wireless infrastructure would be very cool to have, right.  But there's they're up against our regulators, you know, and some other things where historically they've just said no wireless.  But I think even the NRC for us is potentially looking at what those risks are today compared to five or ten years ago and seeing whether or not they can lift any of that in certain circumstances or places.  So wireless for sure is a trend that I see happening as well as AI is in every news cycle, every day anymore. | | |
|  |  |
|  |  | P5 |  | of a nuclear background right now because I've just been at the last ten years or so.  UM, I you know, there's a lot of.  So in nuclear, I'm involved in a lot of advanced reactor research with small module reactors, microreactors, things like that.  And having been a part of those workshops and conversations, they are talking a lot about wireless technologies.  They're talking about using 5G dedicated 5G networks. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 115 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Increasing Dependency on Digital** |  | | | | | |
|
|  |  | P22 |  | Yes, because we're getting more and more and more dependent on electricity and telecoms.  Those two, I mean, that's just it, isn't it?  You know, I I mean I I go walking with a group of retired pensioners and it's amazing how many times the conversation as we walk along turns to software failures and difficulties with the Internet and difficulties with, you know, IT systems that aren't working, you know, so it's, you know, there is nobody who isn't actually impacted by if this stuff goes down or it's difficult to use or it breaks.  Society, but you know it's most people now use their phone to do something which uses the Internet at least once a day.  Now, sometimes you can say you know is there a cost to the economy if you know Pat doesn't get in touch with me about supper? No. But yeah, it's it impacts the sort of quality of life. | | |
|  |  |
|  |  | P22 |  | one weakness, of course, of the.  Of the move to full fibre.  Whereas the old landline, once it's on the main's electricity, they have their own supply.  So we've become more dependent on electricity yet again by going to, you know, BT wouldn't let me have my old phone. I have to have a new crummy little phone. Yeah, because I've gone to full fibre. | | |
|  |  |
|  |  | P22 |  | electricity is the new oil. If the price of electricity, you know it used to be that people talked about the price of barrel of oil. They not now talk about the price of a kilowatt of electricity. And that's the sort of indicator of economic help. | | |
|  |  | P22 |  | Trends are towards more complex as you pointed out interconnected systems. So the trend is going to increase. The cost is only going to go up. | | |
|  |  | P22 |  | Do you see the problem getting bigger over the next 15 years as well? | | |
|  |  | P22 |  | there's a rising distrust of this stuff.  You know? Yeah. God, it never works. Oh, God, it never works.  Which is terrible because you know, like, you know, I came through the IT industry when it was a glorious future and we all thought this was good for humanity, good for society, good for people.  It's turning into a threat. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 116 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Increasing Large Datasets** |  | | | | | |
|
|  |  | P13 |  | . If you want to get absolutely large data, then go to CERN and look at what the large hydrocarli reproduces that that's that's big data in terms of its size.  This is I mean, I suppose what I'd call that, I'd call that linked multimodal data about humans. And I think that's the differences. It's actually bringing together into a coherent consistent.  Structure all different kinds of data and being able to simultaneously make inferences across all of it. | | |
|  |  |
|  |  | P13 |  | OK. And so you see them evolving so so you see a future of huge data. This isn't this isn't big data, this is an order of magnitude more than big data, isn't it? This is something vast. | | |
|  |  | P13 |  | That requires, I think, some particular advances.  Particularly around modelling causal inference.  Those kinds of things.  It's much this data on a much larger scale as well, and the networking has to be there and it has to be fast. But you can see a path to that as well.  You could also imagine as well.  If you have all that data on digital twins.  Would that be enough data to them power?  A transformer model. | | |
|  |  |
|  |  | P13 |  | I think in we're now at the point where actually quite large data sets about people's health are now actually more readily available.  Interlinked and interconnected.  Than they were before. So it means actually, we're now starting to have a good handle or a better handle on how the health system works from a systems perspective.  Through data and so we've had this.  Joining up if you like, of health data and that's kind of grown organically from if you like what we use to serve individual health economies.  That treat populations and then going up to a next level where you get kind of a regional aggregation and we're not really there yet, but that will then go towards the national aggregation and you you'll get insights. | | |
|  |  |
|  |  | P13 |  | Into population level data.  So this is both about I suppose.  By fairly ordinary technologies, to be honest, just increase networking, computer power, nothing really special there | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 117 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Insecure repair or diagnostic technology** |  | | | | | |
|
|  |  | P11 |  | How do we know that this is going to wait?  How do we know that that digital twin is integrity is intact?  Yes, it is it. | | |
|  |  | P11 |  | And the problem with smart sensors? I think that I see is the part for.  Like for like? Well sorry. Like for unlike replacement. So I want a part number 123 XYZ and it turns up and it actually has an RJ45 connector on it and I didn't expect that it's all of the stuff like that that happens. I tell a story of three switches and I put them down. They look almost exactly the same.  Well, they are exactly the same, except one letter in the part number, but one of them has a web server which is really crap. Actually. It's not very well done. | | |
|  |  |
|  |  | P11 |  | Environments like Smrs will only be economically viable if they use technology that isn't currently regarded as being appropriate to those kinds of.  Safety critical environments, so you can't always get the sensors you want and the places you want. You can't always have individual wires going to every last sensor because there isn't the space and they're sealed for life.  So you end up having to do in make inferences to parameters rather than.  Bring them directly. May not be able to measure a particular pressure in a particular place. You may have to make some form of inference.  Using and here it comes using a digital twin.  And and so I see quite a lot now that's that's a sort of development beyond what I referred to earlier, which is that prognostication prognostics and diagnostics there we are.  The prognostics and diagnostics are effectively done, even if they may not be advertised as such against a digital twin.  And I think the question is. | | |
|  |  |
|  |  |
|  |  | P11 |  | I think systems engineer, systems engineering issue, which is related to the use of technology because it's it's stems from that and the use of digital twins in safety critical environments.  You can also see it in the Purdue model, with vendors saying no, no, you don't need a separate card frame for this SIS.  The same controllers in the same car frame as the bpcs. It'll be fine. Don't worry, it's it's it's perfectly OK. Well, I'm not sure it is. | | |
|  |  |
|  |  | P17 |  | I think virtualisation of CNI is something that they're starting to to really sort of get on. I think I think that's where there's a movement to in terms of a technology sort of space because not to say that you can't necessarily replace something with a virtual kind of instance, but.  If you can kind of mimic or or twin it you know with a with a virtualization plane, which obviously does become part of the infrastructure because you need it connected at all times in order to give you real time monitoring and analysis and reproduction of the the modelling of that system. So I think that's something which is is probably not been given too much for at the moment this this kind of additional virtual play which will typically will be cloud based.  But I think that you know that effectively opens up your infrastructure and again becomes another form of well, it just widens the attack surface in my head at the moment. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 118 of 316 |  |
|  | | | | | | |
|  |  | P17 |  | So you know we're looking at at the moment, I mean like for example in construction, you know we're looking at concrete IoT sensors, you know which which you know are going to be these kind of almost these dumb pieces of sensors that you can read. If you put a thing near it, you know like an NFC sort of thing. But I mean if you start looking at things like that and drill down into the fret vectors.  You know, if you're relying on calculations from on a big bridge, which is a safety critical system, you know you you want a bridge to last couple 100 years. If it's, you know, reporting to you that you know that there are fatigues and stresses that are abnormal just because someone's been able to identify that it has sensors and they they rectify the signals it gives off, then obviously that might in, you know, implore a different solution that that, you know might might cause an unsafe situation or it might not. It might just, you know, 'cause.  And and unsatisfactory outcome. Basically, you know you've run, you find out that these sensors are wrong and you know you can't work on them basically. But I think it Edge is definitely a new area that I think CNI is just is going to embrace quite well. So I think that's an area that I think is is is you know somewhere to keep an eye on basically. | | |
|  |  |
|  |  |
|  |  | P22 |  | the lurking danger that xxxalways brings out is that so much critical national infrastructure is built has legacy systems in and they were built to certain standards in terms of, you know, data checking at the front end. And you know now they're being bolted on with lots of add-ons that are brought in from all over the place.  A lot of those systems do not have the same extent of verification of data quality at the front end, and that in fact is the source of a lot of cyber attacks that you know the data checking at the front end isn't happening. And you know there are components built into all sorts of devices that are used in critical national infrastructure that have known vulnerabilities that have been.  In the software.  Incorporates into 260 manufacturers, devices and are now 20 years old and are still there, so there are lots of devices with built in known vulnerabilities, but you know it's not a priority to sort of pull them out because they're working OK, hence the need for AI to record and analyse transient almost failures.  Because we know that there are these buggy devices, these vulnerable devices, these faulty devices in there operating, you know almost 100% but not quite.  And also subject to cyber attacks | | |
|  |  |
|  |  |
|  |  | P3 |  | consequence driven sort of application of technology building defensive architectures on and so forth which you know is shouldn't we should obviously just throw away and had value.  But you know, if we think about kind of machine learning for example and you know an autonomous operation, there are kind of sort of new threats potentially that our existing sort of guidance and best practices are not well covered with by you know what I mean. | | |
|  |  |
|  |  | P3 |  | Because of the danger of interference or. | | |
|  |  | P3 |  | You know, wireless is a technology that kind of is rarely used, let's say in or used with a lot of caution.  In in this space, because you know because of the. | | |
|  |  | P3 |  | And and it's sort of nature of the threat that sort of kind of while you know there's there are additional kind of risks that from cyber point of view that wireless introduces that.  But there's this sort of kind of space. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 119 of 316 |  |
|  | | | | | | |
|  |  | P5 |  | So let let's just take AI or digital twins right now if if people wanna use that technology to help the advanced reactor world for good purposes, great.  But from a security perspective, how do you trust back to the trust?  How do you trust that that digital twin hasn't been manipulated by a cyber adversary to give you the wrong results?  How do you not know that if you're using AI to make decisions to run a reactor that it's not, it didn't make some weird?  Connotations on something and says, hey, today I'm going to operate totally differently. | | |
|  |  |
|  |  | P6 |  | That's the biggest issue. I would say that's that's on the one hand, the biggest challenge of course, when we go a little bit more in detail, it depends on when we come to this safety element, when we are in power plants and if you say critical infrastructure, more production facilities or safety where safety relevance.  Is plays also a role of course.  When we want to apply now AI on it, we have the big issue of how can we apply the advantage in the.  Possibilities of AI solutions in the safety context. So that's a big question mark which has to be worked on. How can we control at the end the black box AI or how can we implement AI models in a safety critical system? | | |
|  |  |
|  |  | P7 |  | so you said transport now and we we we we have some some work there in in in trying to.  Decarbonize transport based on digital twin.  Federated Digital twin technology again, if you have an interface.  Between the physical and the digital twin and you're using one to inform the operation of the other. Anything that compromises either of the two, it has a potentially a very physical manifestation. | | |
|  |  |
|  |  | P7 |  | There is also there is also the the there is also always the the other viewpoint that you know, no, no, no we're we're staying as as much isolated as as we can.  You know are are sort of very good physical security also secures us from threats from the digital. I'm not saying it's wrong.  I'm. I'm just. I'm just saying that there is there is a risk of of missing something because because there is lots of things in systems that are changing.  They're getting they're getting more complicated. | | |
|  |  |
|  |  | P7 |  | So being being risk averse and you know heavily driven by by regulation, meaning that you know change is slow or slower it, it doesn't mean that you're you're more secure.  At the same time, I don't think we should exaggerate the the sort of, you know.  Imminent threat if you like.  But we need to acknowledge that you know the the, the, the more things get connected and you know getting connected might not be an explicit decision, right. If you know, if you, if you're rely. Well, if you rely on devices that you know don't don't do wireless and you wire everything up. If suddenly you cannot find the device without wireless capability.  Your to your net. So I think I think we need to to to to maintain a balance between, you know, scaremongering but at the same time realising that, you know, if if we want to move towards a more a more sustainable economy, a more smarter ecosystem, this means connectivity and connectivity means exposure to to to more threats. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 120 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Integrate Security and Resilience into Software Education** |  | | | | | |
|
|  |  | P11 |  | one of the things that I would do.  Is stop teaching computer security as a separate specialism.  And make engineers and computer computer engineering the words don't fit together. But anyway, making the people who build computer based systems, software, software designers and engineers of other kinds, especially especially systems engineers.  Make them responsible for delivering.  Systems which have a known quantum of resilience. | | |
|  |  |
|  |  | P11 |  | As well as safety, yes. And generally speaking, I think they sort of start to come together. So you end up with systems that are much more.  Designed to be graceful in their degradation | | |
|  | | | | | | |
| **Integration** |  | | | | | |
|
|  |  | P18 |  | Dealing with the consequences should a cyber attack happen, you know that that's that's about human behaviour and about making sure the adequate the processes are adequate. | | |
|  |  | P18 |  | Whereas if you know if you had analogue systems in there, they're lightly impact of a solar storm, probably still impact on the analogue system, but its impact will be different. So the diversity might enable you to be more protected from from something like a solar storm. You know that's just two examples of where that diversity is important and and one of the consequences of the shift towards digital.  Is that a lack of competency?  A lack of competency around analogue systems, so we no longer or we got a very much reduced capability in the UK for analogue electronics.  Because lots of training and stuff goes towards.  Digital. Yeah. Yeah, people coming out of degrees don't necessarily understand analogue electronics. They're mostly dealing with digital things. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 121 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | Yeah. Suppose I suppose knowing maybe it maybe it's competency and awareness as well as behaviour, isn't it? Yeah, there's a risk that the technology and the assumptions around the technology can just take it, bring everyone with them. And that questioning attitude and the behaviour around it is insufficient to make sure that it's all being engineered correctly. So maybe it is Quant, maybe it's twofold.  Is competency.  And behaviours.  I've been doing some work with with IAA and International Atomic Energy Authority around competency and innovation.  And the model that we've come up with is for any application of stuff new.  You need three people.  You need a person who's competent in the technology.  You need a person whose competence in the application of that technology. So. | | |
|  |  |
|  |  | P18 |  | But this behaviour around that, isn't it? You know what's what's a bit. Well, I guess there's processes in there understanding threat actors and all that sort of stuff. But you know, if you've got the right behaviours around it, so which resulting in the right engineering.  You know the right levels of. | | |
|  |  | P18 |  | More you know, experts in you know, whatever you wanted to apply it to and the third person you need is someone who's competent in the.  Process of implementing innovation.  So being that that kind of.  The precautionary principle, you know, knowing, knowing, kind of how you go through the process of developing technology readiness levels and you know the ways of mitigating risk because of that. And I think I think that stacks up an awful lot that between those 3.  Skill sets you can end up with effective deployments of some stuff new, but take any one of those three skill sets away. Then you're leaving yourself vulnerable to either.  Not going down a due process or not having the right level of information on the application or not having the right level of information on the technology itself. So I think that's that's a helpful model to think about.  Those behaviours and kind of competencies around the deployment of innovation. | | |
|  |  |
|  |  |
|  |  | P24 |  | And we we were talking about this in terms of a critical infrastructure that.  We had digital tools. We should.  Give all the responsibility to them to monitor the operation of a telecoms network or the.  Health of a rich if there's the money turns. If there's a sensors in it doesn't say anything is going wrong, then why should I send someone to do the visual assessment? It's not required. I will have extra cost. Maybe if I do that.  And then the issue is trying to. | | |
|  |  |
|  |  | P24 |  | Like transfer these accountability to the tool, which is not actually accountable for that.  For trying to optimise things, but at the end of the day.  A human perspective and a assessment is always required. | | |
|  |  | P24 |  | Yes, tasks. It is required. Maybe not all of them, but there are some that are that someone would should say like Oh yes, this makes sense. Let's keep forward and not just.  Letting these tools run the whole system because then.  There's a higher chance, I believe.  Them failing or us not being aware that it's gonna fail.  Yeah, yeah. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 122 of 316 |  |
|  | | | | | | |
|  |  | P24 |  | There's again, I I don't know. There are many dilemmas with digital tools right now. So in this event that I'm I just mentioned before, some experts.  I agreed with this or they also came up with this thought.  And others.  In the country, they said. So we're gonna have jobs.  That are gonna be four people just sitting, not doing anything. Just put it a in some words.  Because their task is to check what tool does, but maybe they don't even check because they're like, OK, well, it's a done it's fine. Let's move forward. I will still get my.  Salary and that's it. So it was a dilemma.  I think the the the line to draw a line between that is very difficult. | | |
|  |  |
|  |  | P8 |  | Can be designed and integrated the system to human nature I am expecting.  Is to get better because we are pushing for it.  I'm hoping I don't know this my English hoping and expecting are different things I am envisaging it's it. I envisage this to get better because there's more and more progress done in this area right now, so I'm quite positive I'm quite hopeful about this to be honest, because we are now a better systems. We now have a better integrated systems. If we get better, I'm hoping again.  Hop slash XP I hope them to get better. I expect them to get better. | | |
|  |  |
|  |  | P8 |  | Well, hopefully integrated well, yes, I would say one thing that the human factors engineers is we are looking into is a lot of it is integration. This is 3 different type of integration. One is infrastructure to system integration. That is for example you know in an old let's say the truck line or a old rail line. If you put a new brand new shiny train, if you don't integrate it properly it just it doesn't work just because.  So when I say system, please consider in that way system is anything that the humans are interacting with. So in my head a train is a system.  A user interface. It signals a dealing with is a system. A ticket machine that the passenger is dealing with a system. So when I say system, I mean all of it. So integration of infrastructure to any system is where the changes will happen and popping will happen. We are pushing for this to happen so things will be more safer, efficient and effective system to system integration that means.  In a control room or where the drivers or the passengers look, there are six seven different type of systems right. There is one computer here, one CCTV there. One thing there are they.  Integrated. Are they all usable? Are they all intuitive or are they confusing the hell out of human being and increasing their workload? This is why we are coming in. Workload could be for the operator, workload could be passenger workload. If I'm trying to check in and you give me 15 things to integrate with just because you didn't consider.  The systems to system integration I have a problem with it, right? So this is second one system to system integration. The third one is very important is human to system integration, right? So you integrated the infrastructure with the system perfect. Well, fine. We integrated all the systems to all the systems perfectly fine. OK. But you did it all for the perfect human, which sometimes engineer tend to do,  And the perfect human is, you know, young, able bodied, capable.  And 10 ages no, I'm sorry. The humans come in all shapes and forms. We are not all that intelligent. We are not all that we know. For example, you know, we are not all that young. We are not all not disabled, you know. Like I'm changing. And that might develop like an understanding and dealing with things change like as I get older. 20 years ago I could be faster than I'm not. And in 20 years I will be even less because it's just human nature human nature. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  | P8 |  | Well, you said how you see them evolving and changing the sector in the next 15 years, so so a more integrated. Are we talking about then sort of more more integrated with other travel services and? | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 123 of 316 |  |
|  | | | | | | |
|  |  | P8 |  | It could happen, although this might be looking into human factors because you know the humans will not change that fast. We will always hear people who are a bit older. We will always hear people with disabilities. We will always have people who don't like technology, so I assume they will not be fully automated, but some kind of game changes. They could be that around the stations from the passengers point of view, I could imagine that and also the touch points what we call is RAD.  They say the passengers leave a pass or a taxi or the tram, and then they travel to the station. There could be more.  So this process could be more streamlined. I think the process of door to door travel door to door, I mean from the house to wherever you've been to get to, I think there's a lot of game changes in between of those interfaces. So not in one place, not in a control of another, not on a train, not on a station. Not a lot but a lot of that thing changes will happen in between which doesn't look like.  A real network, but I think from the door to door journey point of is a railway network.  Angle affidavit. Yeah. Thank you. | | |
|  |  |
|  |  |
|  | | | | | | |
| **Interconnectivity - interoperaility** |  | | | | | |
|
|  |  | P12 |  | Anything that has has to do with CDN failure can mess things up, so you have misconfigurations. I mean this happens. This happens not infrequently, but like Acdn, will this configure something and like all of their customers go down? Of course the problem is even people who are not directly their customers may be rely on a font or a JavaScript library that is hosted by one of their customers. And then that thing goes down and causes this cascading failure. So yeah, misconfiguration of Cdns I mean. | | |
|  |  | P13 |  | I mean it it it's hard to separate things out because I think actually there's a high degree of interrelatedness between a lot of things, but.  I think perhaps.  Looking at this as kind of a continuum, I think in we're now at the point where actually quite large data sets about people's health are now actually more readily available.  Interlinked and interconnected.  Than they were before. So it means actually, we're now starting to have a good handle or a better handle on how the health system works from a systems perspective.  Through data and so we've had this.  Joining up if you like, of health data and that's kind of grown organically from if you like what we use to serve individual health economies.  That treat populations and then going up to a next level where you get kind of a regional aggregation and we're not really there yet, but that will then go towards the national aggregation and you you'll get insights. | | |
|  |  |
|  |  |
|  |  | P14 |  | As more systems become connected.  There is greater complexity. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 124 of 316 |  |
|  | | | | | | |
|  |  | P14 |  | And oh, and the other thing I should have mentioned, of course, is the Internet of Things is another major game changer, because when the whole world is connected up.  And when you could actually, you know, a sort of some some spotty youth in a basement in Melbourne just wanting to have fun, not necessarily trying to destroy an enemy, but just wanting to, you know, have a little bit of a laugh.  Can connect through and get into some Internet of Things link which then breaks into a bit of the critical national infrastructure. You've got huge challenges there, so when you get the democratisation of technology and capabilities that quantum might offer, it won't initially, of course, but might eventually offer.  Certainly with Ji and ML does offer combined with an Internet of Things which allows everything to be joined up in a. | | |
|  |  |
|  |  | P14 |  | And | | |
|  |  | P14 |  | And I mean you, you, this is this critical challenge, critical risk management challenge around systemic failure where you get a knock on effect. One thing fails and isn't very significant, but it has an impact on something which is far more significant and understanding.  The complexity of that.  3 dimensional world.  And all the potential links, feedback loops and everything else is hugely important issue. | | |
|  |  |
|  |  | P14 |  | Passed away than ever has been possible before. You suddenly have an attack arena which is vast and with huge numbers of unidentified potential threats in terms of players who can get into that attack arena, you've got some interesting challenges there. | | |
|  |  | P15 |  | AI and computer technology like is the risk that is is worrying in terms of or it's it's an unknown and it's the interconnectivity of the sort of asset management systems and data management systems and all of these things are sewing interconnected that if you have a failure in one and sort of not being able to understand in advance what the ripple effect would be on those systems.  And I think that the more things are automated, the more things rely on on additional technical systems and technical solutions.  Then it's sort of increasingly interwoven with each other and then becomes increasingly difficult to understand.  Where that happens. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 125 of 316 |  |
|  | | | | | | |
|  |  | P15 |  | Oh well, I think they're generally running them. I am less well versed on because that's, I would say that's the day-to-day technical management of those systems.  From a generic sense of what you want technology to do in an emergency, it's predominantly around sharing and like situational awareness. Understanding what's going on, so knowing.  Well, from the whole sort of risk management cycle of being aware of what risks there are and having using technology to inform your understanding of either existing risks and how they're changing novel risks and what.  The impact of them is going to be on your, on your systems, on your critical assets and on your processes that you're trying to protect and then using that information for situational awareness to realise when things are actually something is about to happen or something has happened and having an ability to recognise that and then using that situational awareness to inform your response. So being able to activate the right responders, being able to share information with the right partners and then to be able to sort of maintain that situation, that situation awareness as the incident is being responded to.  And then afterwards. So I think if you think about technology informing each of those different processes, I think.  There's a lot of opportunity, potentially both to do that badly.  For somebody with malicious intent to try and disrupt the information flow, so either to prevent you from knowing that something something is happening to be creating a risk.  In terms of cyber threats and things like that, but also to disrupt your ability to to collate information, I think there's also just a sort of not even from a malicious intent perspective. | | |
|  |  |
|  |  |
|  |  |
|  |  | P15 |  | And I also have the benefit of just sort of swanning in and telling people good things and then swanning away again. I'm not responsible for any CNI. Think if I were, I would probably have different.  What keeps me up at night?  But also so then again.  If we're being really honest, it's what keeps me up at night. Is there aren't enough emergency planners doing things because there's not enough funding? Certainly.  I would say not necessarily in commercial entities because I don't know that so well, but the.  I would say it's a greater a sense of how.  How different organisations that are multi agency perspective are able to operate together.  So any kind of major instant response or major emergency or disaster response is never going to be just a single agency working on their own. | | |
|  |  |
|  |  |
|  |  | P15 |  | And I think my kind of fears are we might have been in a good position X number of years ago.  But things are being like eroded quite a lot, and therefore people know stuff should be being done, but particularly in the health services and local authorities and and police and stuff, there aren't enough people doing it, even though they know and the people who are working there are are working under very different pressures. So I think it's probably those.  Like resourcing and funding kind of issues because they underpin literally everything that you're doing. It's all well and good saying I'm, I know I'm really worried about the situation in Ukraine, the impact that's having on fuel, the fact that we're like quite likely to have.  Major fuel issues if we have significant bounce of cold weather, we're going to run out of fuel and and we'll have issues around that. But like there.  They're sort of risk specific. I think I'm probably more worried about the more general context of.  How everybody works together in in a bigger sense, political direction in major incidents.  Which can be erratic at best.  And and their engagement in emergency response in advance of the incident. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 126 of 316 |  |
|  | | | | | | |
|  |  | P15 |  | Is if you look at the technological systems that support emergency services response and interoperability.  There are already challenges when it's working well because you're working with people who aren't necessarily like technically proficient in that way they aren't normally used to doing XY and Z, and this might not be at the forefront and therefore it's a sort of training and exercising and skills fade thing of OK, don't normally have to engage with this system very regularly, and I've forgotten how to use it. And now X has happened and the the plans that they need to do Y and I can't remember how to turn this thing on or I don't have the password like like you would be amazed how much like with the really basic stuff.  Goes wrong.  And therefore I think anything around making, I think there's a potential for.  Comms and information sharing and technical information sharing.  For situational awareness and response and decision and making good quality decisions based on as much information as well, not as much information as possible, can source it possible to get overwhelmed by information, but normally you end up not having enough and then you have too much of it.  And therefore, like there's a, there are opportunities I think for technology and technological advances to.  To aid those processes, but there's also quite a lot of opportunity for unintentional, unintentional errors with those. | | |
|  |  |
|  |  |
|  |  |
|  |  | P15 |  | Not necessarily. Always complexities for some people that might be complexity. For some people that might be extra information that they can use. It depends what it is that you're trying to decide and what you need to what you need to how much you need to have to make that decision. So then we do end up straying into my my PhD research around like how people go about understanding and making decisions and.  How? How you even go about making knowledge and when you get overloaded with things like that?  So I think it it all depends on who you are and what systems that information and data and knowledge is sort of circulating in who has access to it.  Because the ways that the ways that these technical systems will be structured will be creating other other boundaries and gatekeepers and new spaces for things to happen and New Times when things happen because the system requires updating on a regular basis and when you're doing that by paper or some other non not as advanced technical way.  You might have a different like timings and spaces and access rights that are there for those things will manifestly change the relationships people have with that data and how they how they get access to it, who they share it with, what they can share the the literal way that it is visually represented. | | |
|  |  |
|  |  |
|  |  | P15 |  | There are lots of technical systems by which people store information.  And I think if there were ways and I know people have been looking at this and how to make those systems interoperable and be able to speak to each other so that you can, if you if I as organisation X have this very important information, I'm able to share it with organisation, why it takes into account GDPR and and data sharing.  Legislation as relevant.  And then you receive it in a way that is meaningful to you.  And and make sense to you and you're able to do what you need with it, so I think. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 127 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | Well, it's it. Well, it's it's a it's it's a very I mean it's not. I'm not claiming it's something very complicated. It's just like the fact that when you have those interconnected interdependent systems and you have like a very autonomous tools now being developed to attack or to defend. So you have machines that are making decision just like in the stock market when you have an initial, you know, a tiny event.  Generating a cascade of decisions.  Decisions by, you know, in microseconds by.  Software that is trying to beat the crowd. So I think that's why we're probably going to see when when AI is going to be manning a lot of our cyber defence systems and AI are going to also attack and are going to let loose by malicious actors to attack certain targets. It's very possible that.  You know, they didn't think of all the implications and the the attack might get out of hands and and and keep on propagating outside of the initial bounds of what was planned or envisaged. And we end up with, I think the.  What's the? What's the attack that you know what? There. What's what's happened with the Russian malware?  Can't remember one. I cried, so not pity. I wanna cry 2 pieces of malware that were supposed to be contained to attacking Ukrainian.  Organisations. But because of the the fact that a lot of Western companies had outposts in Ukraine were operating in the Ukraine, then it was used. | | |
|  |  |
|  |  |
|  |  | P16 |  | You know the the the, the system replicated and just kind of.  Went a wire and just went all all around the world and paralysed a lot of companies so that that's the idea of propagation. You know you have something in mind that may be a very contained attack. But then because you it's becoming so complicated and so complex. Even for the goodwill attacker, you know it cannot understand all the.  The complexity of the whole ecosystem and might just produce results outcomes that they never kind of actually wanted to to achieve. So that's that's you know this kind of propagation, something that gets out of control.  And not because someone wants to pose major havoc, but just like they didn't think through exactly and they didn't have a clear map of the interconnectedness of our digital ecosystem.  Exactly. Exactly. | | |
|  |  |
|  |  | P16 |  | Yeah. So yeah, so there's a, there's a. There's a reason why this is going to may well get worse. And it could even be dealt with by human negotiation, you know, iPhone you up and say by the way, you do realise that you are, you know, you're going to, you're going to make us both look bad. But by doing this, but we've got to know to do that. Yes. Yeah. | | |
|  |  | P16 |  | Yes. And the and the fact that because we are interconnected but still distant. So if we're interconnected through two or three degrees of separation.  Your future is of no concern to me because I'm not gonna be the one who's gonna pay the price of my decisions being propagated to you and crushing your system. I'm gonna say too bad, so sad. But you know, my incentives are zero, so I'm gonna keep on doing what I'm doing because it.  Serves me even if it weakens you. So those kind of emergent effects when you have negative externalities that I'm pushing to you and you may not have the label of sophistication to understand or to absorb that I'm saying, but that's not my problem. You know my decisions, my systems are perfectly safe because of my decisions, maybe it generates discomfort for you, but fix it on your on your end, you know.  It it may, it may work from my perspective, but from a system level perspective, it's kind of disastrous because it it it generates.  A system where.  No one is looking after the negative consequences of their own decisions, so that's making sure that we generate at the system level.  A way to regulate not only individual decisions like my decisions, but also the emergent effects that kind of negative emergent effects that are not my fault directly I I have got no I'll intent against you. It's just that because I'm not incentivized or not regulated, I'll keep on doing what serves me when I should also kind of maybe be made aware of the negative impact on you. | | |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 128 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | Yes, yes. And we so we we need a even to be able to to know who to phone you. You need maybe to have like.  A A platform of trust from which we can communicate to each other. What what I am doing to you without necessarily kind of wanting to attack you. But what my decisions are doing to you and try to solve it together. So we need to develop.  For us, where we can discuss this and we can try to fix it together.  So that the overall ecosystem stays healthy. | | |
|  |  |
|  |  | P16 |  | It's the the political scientists they call that a trans boundary crisis, because usually, you know the the people like us, you and I, studying crisis. We're usually studying a specialised in this in a in a in a discrete area of human activity. So I'm a criminologist. I'm interested in in fraud. People are working in different sectors. But now because of this interconnectivity, different sectors are.  Connected to each other and they operate under different assumptions and they have different cultures and they have different.  Frameworks in place and when the crisis crosses a boundary, then it transforms and it is being made sense of using different tools and it's becoming difficult for people from different areas to communicate with each other because their mental models are different. So that's so that's, you know, those are the different variables that explain why this is.  Introducing.  Complexity of risk, that is that are not that is not as easy to handle. Then the more conventional crisis contained documented, more predictable, easier to respond to, and and so on and so forth.  Yes, yes, yes. | | |
|  |  |
|  |  |
|  |  | P16 |  | Yeah, negotiate. I mean, you use the term negotiating something. You know, it's the the comments, you know, when you when you leave under a a comments system you know we you have to jointly agree with all the other users of the comments that you're not going to over exploit you're going to be and I think this is the kind same kind of.  Configuration where we need to be able to discuss and then to agree and then if we can't agree together, someone has gonna step in, has gonna to have to step in and probably the state and to say no. Now if you can't agree it's it's better if you agree together without enforcement or without and you coercion because it's very often introducing it's on emergent effects that are very often and desirable as well. But if you can't agree for a reason or another then I'll step in but.  Let's try to have a joint.  Discussion or negotiation among reasonable people or stakeholders to ensure that we understand how this interconnectedness is impacting everyone and how we can address it. | | |
|  |  |
|  |  |
|  |  | P18 |  | Again, that goes back to that interconnectedness said at the beginning, doesn't it? You know that if you, if everything's interconnected, then the potential for one to have a negative impact on the other. And that's a kind of promulgate and just you end up with with difficulties and and and I suppose.  With. With that, it's the ability to recover that becomes important so that if you, if everything's interconnected and so it starts.  Doing its thing its its thing. This often is you know very difficult to stop that propagation of the issue but so it becomes a function like the impact becomes a function of your ability to recover, to stop and recover.  And I don't know whether that mindset.  Has has has been, you know is is common, so it's it's common in cyber security isn't it? You know, recoverability from a cyber attack is an important concept.  And I know that for things like blacks, black start on the grid, you know, it's becomes really important and that and and that black start is you know how do we recover from a kind of mass blackout and kind of what's the time scales what's the process so that that recoverability I think is an important aspect.  'Cause I know what it was gonna or what I was gonna say before. In all of these cases, I think it's helpful to think about modern technology. You know, when think about the likelihood of things happen happening, like in failures, the likelihood of failure is 1. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 129 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | Including the people. Yeah. Yeah, yeah, yeah. Yeah. So and.  And in yeah, that that to some extent.  Picks up on that interconnectedness, you know, and and and.  Yep. So we've got something really complicated or complex rather, and it's gonna have an impact on something if let's not, let's not just stop there. Let's think about the knock on effects of that. So yes, it's a whole system's view rather than thinking too narrow. Narrow. I mean, there's a limit, isn't it? Because you could end up with everything being the same problem. So. But, you know, thinking beyond the technology I think is important. | | |
|  |  |
|  |  | P21 |  | It goes a little bit back to the workshop discussions now. It's still we that can come up there. I thought I wasn't quite convinced by that. I think in some ways that sort of easy to think that interconnectivity is necessarily a bad thing. But I think it can also mean that some things are more secure or you're sort of if you become part of the sub network, you might for example have to meet there already higher requirements. If you think that you are now acni provider then.  Maybe that means you have to.  If she and I provided might be more sad and mature, and their hygiene and then you might have to meet those the same requirements. So I don't necessarily think that that's the case, but I think in some instances, for example, schools where more interconnectivity has been done instead of. | | |
|  |  |
|  |  | P21 |  | Small steps over a long period of time with very little systematic effort or budget or knowledge, really like I don't want to blame the school for that, but that's just how things developed as well in universities.  In those instances, I could see how that that can be become a problem, yeah. | | |
|  |  | P21 |  | Yeah, I I think it depends on how interconnectivity is is achieved.  If we just randomly plug in more things without understanding where failure points are or where where more measures are needed for example, then I think yes. But.  Per say, connectivity isn't isn't a bad thing.  Yeah, I think it's more. | | |
|  |  | P22 |  | Well, it's it's connectivity.  But the the.  No, I can't use the phrase in the wood part, but the the lurking danger that xxx always brings out is that so much critical national infrastructure is built has legacy systems in and they were built to certain standards in terms of, you know, data checking at the front end. And you know now they're being bolted on with lots of add-ons that are brought in from all over the place.  A lot of those systems do not have the same extent of verification of data quality at the front end, and that in fact is the source of a lot of cyber attacks that you know the data checking at the front end isn't happening. And you know there are components built into all sorts of devices that are used in critical national infrastructure that have known vulnerabilities that have been.  In the software.  Incorporates into 260 manufacturers, devices and are now 20 years old and are still there, so there are lots of devices with built in known vulnerabilities, but you know it's not a priority to sort of pull them out because they're working OK, hence the need for AI to record and analyse transient almost failures.  Because we know that there are these buggy devices, these vulnerable devices, these faulty devices in there operating, you know almost 100% but not quite.  And also subject to cyber attacks, because you know, if you've got good enough defences at the front end, the cyber, the, you know, malignant attacks. Sorry, I'm. | | |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 130 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | You know, all stuff that's nice and implementable using Python, so the sort of implication of that kind of is that the sort of from an adversarial point of view, your ability and neither all open standards.  Of course, from adversarial point of view it makes it a lot easier for you to to sort of.  Yeah, to kind of like learn how to manipulate these systems, right.  You know the the implementation becomes a lot easier all of a sudden because you don't have to understand some obscure SCADA systems scatter protocol right to do that.  And I think that kind of that, that sort of Internet ification, let's say, of industrial control systems that are underpinning all of our CNI is, is, is, is, is something that's you know on its way and and well well underway I think which has sort of implications from a I think from a risk point of view. | | |
|  |  |
|  |  | P3 |  | So the way that, at least in in in Europe, and I suspect it's it's similar here because I I don't know awful lot of opportunity to kind of engage with dnos in the UK just yet.  But so one of the main ways that sort of distribution system operators sort of interact with substations is via protocol, let's call it IEC 61, something something 104, right?  It's just abbreviated to IEC 104.  Normally this is a sort of very classical kind of uh SCADA supervisory control and data acquisition kind of protocol that's used to sort of get, you know, inform, you know, remotely collect information from substations and apply control and stuff like this.  I'm so and that kind of, yeah, sort of traditionally been a little bit sort of difficult for an adversary to sort of understand and reason about us changing a little bit and maybe we could talk about that and but if we look, if we sort of look at electric vehicles, so it was involved in a project that was sort of looking at electric vehicle cybersecurity before, before I left Vienna and there's sort of the protocols that are being used to, umm, manage charging stations by charging point operators and stuff like this a basically it's using web.  Technologies, right. | | |
|  |  |
|  |  |
|  |  | P3 |  | So so the the sort of you know, the the classic story there is that you know it all started with this idea of having prosumers, right, that have some sort of interface to the energy distribution, the distribution system operator or the DNL is, I think the called here in the UK.  Then it's like sort of, you know, energy service providers of different source doing things like demand response and they sort of signal into you know basically there are kind of relationships between these entities to make sure that we have frequency at 50 Hertz voltage stays within a certain band.  You know, I sort of interfaces onto the energy market as well.  So they're basically the whole thing gets a little bit like I say, a little bit more open.  There are kind of more say programming interfaces or API's that that kind of exist to sort of realize this sort of vision and this in connect interconnected grid and then sort of there are kind of new communication protocols that are being used.  Some of these are sort of, uh, more Internet like in their kind of operation, which is a sort of departure, I suppose, from from the way that these sort of.  Systems operated in the past just to give you an example. | | |
|  |  |
|  |  |
|  |  | P3 |  | And if you're using digital systems to support remote surveillance, physical protection systems, or this kind of stuff as part of a blended attack, then theft of material is becomes a bit of an issue.  And then the other kind of sort of potential shift in and kind of concern is around availability, right, energy security, right?  So if we if we, if we don't, if we can't necessarily, you know maybe we don't.  Our attacks don't result in, you know, release of material or anything, but we could put the thing off off grid, right offline. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 131 of 316 |  |
|  | | | | | | |
|  |  | P5 |  | OK, that's one of the things that we talk about in cyber informed engineering is complexity versus simplicity.  And one of the recommendations is to make it as simple as possible to perform only the function that you need it to perform of the system.  So for instance, you buy a programmable logic controller.  It may have two or 300 functions that it's capable of.  You basically configure the five functions that you want it to do for your process, and then all of those other hundreds are there.  If an adversary gets into that PLC, they potentially can enable those and do things that it wasn't designed for.  So our push is, if at all possible, remove all those other hundred functions out of that PLC, if that is possible.  The bottom line is you only want the system to perform the functions it's supposed to. | | |
|  |  |
|  |  |
|  |  | P5 |  | Of course, of course, because now you're essentially connecting different functions together.  Through these networks and things like that, so that and also to gain access, you know original access, you might be way down at the very end, but if it's all connected, you just pivot your way through these systems that we have proven over and over again to get to the final system of interest.  So yeah, interconnected.  That's why we talk a lot about defensive architectures and segmentation, where you segment these things so that no one can get to those critical systems.  So yeah, that's definitely a big one. | | |
|  |  |
|  |  | P6 |  | There is no producer which doesn't need additional data to improve the efficiency of his production process to to manage the the the supply chain, whatever it is that one needs at the future one meets weather data to improve his accuracy machine the other need other dates to compare his production data. So we are starting to exchange data very much in this machine context.  Very much also in the private context as personal human beings, either to create big data applications.  Look, I don't know a situation on streets. We don't need individual data, but we need many data. That's or we create AI, whatever it is of the behaviour analytics of people. So it's everybody produces data and we are shifting it around and also for the critical infrastructure. However, we will define it. So for metric providers, PowerPoint power generators. | | |
|  |  |
|  |  | P6 |  | So there is no supplier which sells his product to anybody without remote maintenance. | | |
|  |  | P6 |  | So yeah, and and and and this this problem even goes further when we come to the to when we try to prevent our critical ITOT infrastructure and we are applying AI for anomaly detection, I think which is a good illusion and we should go for it and researchers and they're working on it. So there are. | | |
|  |  | P6 |  | But of course, as soon as you're building it, you indent the system is identifying something. That's the starting point. That's again talk about complexity. It's a starting point because the system doesn't know, and you you as user of operate of the system, do not know. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 132 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | Is it now a failure in the system, or was the external attack you're you never know, so you get much more information you need. Again, more powerful IT systems which are sorting out this information that at the end you come to a kind of decision mode. So just applying AI is a very cool idea as a sensor, but it's not yet the solution. Solving all the problems we have to build on it and to build much more powerful system.  As we said at the beginning to master it.  And this question, accident or failure and remote attack will always be there. We have to find means in there, of course.  I got you. I got you | | |
|  |  |
|  |  | P6 |  | The the big momentum on a strategic principle level, what we have to discuss are for Me 2 elements. On the one hand, it is the overall interconnectivity. So we have more or less full interconnectivity among all human beings, everybody, a smartphone, a tablet. So everybody's connected and we are now.  A very active globally in doing interconnecting the next group of the next market or group. We're connecting all our technical system so call it now industry for the 5:30.  Everything is will be connected with everything, so we are we are building this full connectivity. So that's for the moment we have to deal with the people connectivity. The next challenge which is not yet there.  Is this machine to machine connectivity, so that's still going on. The next element, which is the next decade, which I think is now crucial. What we are just starting globally is building on this technical platform. It is there now everywhere you have IT. So that's for mediaturization. It's a full connectivity. Everybody can in principle reach each other. We have connectivity and in each.  Moment. What? It's a sensor or a powerful computer. Whatever it is, we have a piece of software. So that's these. Two parts are now. That's what that machine machine can communicate. And all this stuff. So this system is now generating the platform of the new would say data economy, which is now starting. And this is not yet. No, no, no, even not completely. That's not yet understood at all. That's one of the biggest problem from a business perspective but also.  What should we do? Whatever we means we as.  Authority as a, as a strategy advisor, as a leading framework builder, or as an industry actor so that the economy the system is now starting enabling for the moment. We have owned a handful main actress and we are talking about our cloud services. | | |
|  |  |
|  |  |
|  |  |
|  |  | P6 |  | Then we are in the supply chain. The supplier has to do it after responsibility for data and so on.  Nevertheless, the system becomes very complex and I think compared to 100 years ago, or even, I would say 20 years ago, the time that there is one engineer which understands completely and can describe his system, it's gone even without AI. So it has nothing to do with AI. It's gone. It's overall unbelievable, became complex and nobody can oversee it. The world system, when AI comes into this, into the game as models, even then even more, you can no longer that the Minister can describe it.  So we have an unbelievable or an an enormous growth in complexity that's that's a big threat on the system. And since it's about software development.  We will always have our vulnerabilities in there.  And when we now accept as a threat model that we can discuss about philosophical way of political systems and human beings, there are plenty of threats out there which we see every day now on on the TV, there are always other people from crime to terrorism to state actors which will use.  Those vulnerabilities in our great infrastructures that we have very complex systems. So in Europe, we are answering now with increasing regulation and laws like NIST two and the Resilience Act. I think I believe it's a, it's a huge burden on the manufacturers and suppliers.  But I believe it's necessary that it's done, otherwise we will end up in a big mess. But nevertheless the question is, are we able to manage it? I mean, just having a regulation or law is something, but you have to enforce it, you have to.  The manufacturers to be able to implement it, we do not have laws that somebody's paying fines. We have lost the system's become more safe and more secure. So the question is, do we have the know how the people, the tools to build the system even we have laws out there to put the system much more resilient. And I would say I said before as a summary when it's even a management summary that we have from infrastructure to communication this data level now. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 133 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | Also, a very general statement.  It is true for any IT systems, but also of course also for critical infrastructures. | | |
|  |  | P6 |  | Due to the digitalization and connectivity.  And using services and all this stuff.  Any IT system becomes more complex, so we are increasing dramatically complexity. Of course we are outsourcing a large extent. So for the stakeholder becomes easier because I'm outsourcing it to a cloud provider to service provider of course. But outsourcing doesn't mean that I get rid of the security responsibility so | | |
|  |  | P7 |  | So being being risk averse and you know heavily driven by by regulation, meaning that you know change is slow or slower it, it doesn't mean that you're you're more secure.  At the same time, I don't think we should exaggerate the the sort of, you know.  Imminent threat if you like.  But we need to acknowledge that you know the the, the, the more things get connected and you know getting connected might not be an explicit decision, right. If you know, if you, if you're rely. Well, if you rely on devices that you know don't don't do wireless and you wire everything up. If suddenly you cannot find the device without wireless capability.  Your to your net. So I think I think we need to to to to maintain a balance between, you know, scaremongering but at the same time realising that, you know, if if we want to move towards a more a more sustainable economy, a more smarter ecosystem, this means connectivity and connectivity means exposure to to to more threats. | | |
|  |  |
|  |  | P7 |  | Yes, and but also there's a really interesting suggestion what you're saying there that whether we want it or not, it may be the only economical option.  If only because you know every single device will have a, you know, a Wi-Fi connection and and trying to do the non Wi-Fi version is going to be you know it's going to be ridiculously expensive.  Yeah, yeah. | | |
|  | | | | | | |
| **International Coordination** |  | | | | | |
|
|  |  | P9 |  | successful the seeds of our success are sown in our own her own destruction, the mechanisms that will enable us to respond to these systemic threats are in the same free flow of information, digital engagement that we've created. We need to make sure that it's light side wins out over its dark side. | | |
|  |  | P9 |  | how you collectivise and delegate.  Your your decision making and what is the right level of body at which to make those decisions and then you know communicate and commit to them and our our supranational bodies are ineffective for various reasons and always have been. But some of these issues are bigger than the nation state and they need to be addressed. And so the the corpus, if you like that manages that then becomes.  Culture and society, so it's a public narrative | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 134 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Internet Standards Make Hacking Easier** |  | | | | | |
|
|  |  | P3 |  | Of course, from adversarial point of view it makes it a lot easier for you to to sort of.  Yeah, to kind of like learn how to manipulate these systems, right.  You know the the implementation becomes a lot easier all of a sudden because you don't have to understand some obscure SCADA systems scatter protocol right to do that.  And I think that kind of that, that sort of Internet ification, let's say, of industrial control systems that are underpinning all of our CNI is, is, is, is, is something that's you know on its way and and well well underway I think which has sort of implications from a I think from a risk point of view. | | |
|  |  |
|  |  | P3 |  | SCADA supervisory control and data acquisition kind of protocol that's used to sort of get, you know, inform, you know, remotely collect information from substations and apply control and stuff like this.  I'm so and that kind of, yeah, sort of traditionally been a little bit sort of difficult for an adversary to sort of understand and reason about us changing a little bit and maybe we could talk about that and but if we look, if we sort of look at electric vehicles, so it was involved in a project that was sort of looking at electric vehicle cybersecurity before, before I left Vienna and there's sort of the protocols that are being used to, umm, manage charging stations by charging point operators and stuff like this a basically it's using web. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 135 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Isolated - Close Systems - fragmentation** |  | | | | | |
|
|  |  | P10 |  | So we have the national, you know, cyber strategy. We have the government cybersecurity strategy, every country is coming out with its own strategy at the moment. Good, good on them. Some of them are also coming up with some very narrowly focusing on cyber here. Some of them will say very sensibly coming up with their own action plans. We don't yet have one in this country.  MAD are coming up with their own strategy and action plan. The National Health Service is coming up with its own strategy. You see where this goes. So the fragmentation across the piece, I mean, just as I'm critical of monoculture for obvious reasons, I'm also critical of, you know, abject fragmentation and siloisation because we really do need a joined up approach here. And so that that's that's, you know and and some very strong leadership and not getting quite so distracted by shiny things like AI.  But you know, actually thinking about this and I I sort of mentioned that that kind of shift in gear from.  You know, to, to, to you know, to to a dangerous time. I mean, I think it's we've always been living in dangerous time. Right. But I think you know that it's not as safe. It's not. The world is not a safe place for the geopolitics. Engaging, engaging here. Not not.  Not just focusing on the geopolitics, but, but you know they they obviously kind of setting setting the scene here. But I think you know some some real direction, some some.  You know, there is so many different agencies in in the UK in particular leading on this and then globally it becomes even more, you know, even messier.  So it's very easy for you know, the tech Bros to to do the thing that they want and we have we spend very little money comparatively on on this. So that those those I think are are are key considerations here. | | |
|  |  |
|  |  |
|  |  |
|  |  | P10 |  | Exactly. But I think it probably it should be, yeah, that sort of thing, you know, so I I just just something that's kind of Co ORDINATED doesn't have to be you know I'm I'm not I'm not you know I'm not I'm not overly invested or you know in my in my trust in in in the ability of the government to deliver on important things here shall we say you're my cynicism was clear when we started but I I think something like that would you know making it whole of society approach that's that's globally would like to kind of push on say bringing in industry you know people are throwing far more money on it in in business initiative than they are able to in government so.  What? What are they learning? What can they share?  Academia again, you know some some great minds and some great work, you know, get those people around the table rather than that, the fragmentation that we see at the moment, with everyone doing lots of, you know, a lot of busy work, how could we join this up and be more than some of our parts? I know that's a terrible cliche, but I kind of think this matters. | | |
|  |  |
|  |  |
|  |  | P10 |  | So you see this as a as as the best thing to be some sort of global. So some sort of UK wide.  Strategy and actual plan from it to to address the resilience issue as much as anything. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 136 of 316 |  |
|  | | | | | | |
|  |  | P23 |  | There's like there are very very basic things like her.  Have you can have you allowed your control infrastructure to be connected to an Internet?  Resource like the most basic A that are not fully ironed out and the attacks against these infrastructures tend to be really basic stuff, not quantum stuff.  I'm gonna find you on LinkedIn and I'm gonna send you an email and ask you to log into the control site or the other.  So it it we really are at at our infancy and and and one of the questions, one of the great questions out there is why why haven't we had a disaster?  Umm the and there is some speculation, you know, like why haven't we had a dam loose control and kill 1000 people and the there is speculation that in fact many of these institutions do not but the you know the larger ones have not connected their control to the Internet and and so on yeah another reason is that many of the infrastructures are quite old and that and the way makes them difficult to attack because no one knows I mean I mean I know Web programming languages but I do not know Fortran and so on. | | |
|  |  |
|  |  |
|  |  | P23 |  | So the needs of the different stakeholders differ a great deal.  There are more and less sophisticated stakeholders.  And I'm sorry that this runs a bit against your that the kind of motivation of your study, but these bodies don't need protection from quantum computers because they're not even ready for basic cyber security. | | |
|  |  | P4 |  | You know the sort of morachi the Maroochy Shire attack, but you know, people didn't really think about that when the infrastructure Moroka share MRO's MAR double OC, HY, if you just Google it, it's like considered like the seminal attack on on water systems. | | |
|  |  | P4 |  | So | | |
|  |  | P4 |  | And one of the things that I remember speaking when this is all when Stuxnet was actually happening and I was speaking to people who were who were working at these plants and they said, have you heard about Stuxnet and went?  No, no, that was just something we should sort of worry about.  And you know, we'd, we'd ask them.  What would your security you know?  Are you worried about, you know, attackers trying to come in and corrupt cool PLC to try and make your trying to make it do things you shouldn't do?  And they went no. | | |
|  |  |
|  |  | P4 |  | Well, not really.  They kind of isolated systems, you know, I mean you you you could cause harm, but you know, you really would have to go out of your way.  And why would you wanna?  Why would you want to attack this particular wastewater treatment plant with with clean water is a little bit different with clean water.  The police are a lot more alerted into them, but you know, a typical sewage plant. | | |
|  |  |
|  |  | P4 |  | Plants are just overloaded water and ends up waste.  Sewage ends up in the sort of river.  So that sort of things, you know, and that could that could cause harm. | | |
|  |  | P4 |  | You you could cause harm because they're they're worry was actually if you know much about water courses, the removal of so much green space means that a lot of water now floods into now actually goes into sort of drains.  And you know if if you get a lot of heavy, if you get a lot of heavy rain, you get wastewater treatment path. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 137 of 316 |  |
|  | | | | | | |
|  |  | P7 |  | I mean, I'm sure there is. There is also there is also the the there is also always the the other viewpoint that you know, no, no, no we're we're staying as as much isolated as as we can.  You know are are sort of very good physical security also secures us from threats from the digital. I'm not saying it's wrong.  I'm. I'm just. I'm just saying that there is there is a risk of of missing something because because there is lots of things in systems that are changing.  They're getting they're getting more complicated. I mean, you know, did. | | |
|  |  |
|  | | | | | | |
| **IT to OT** |  | | | | | |
|
|  |  | P11 |  | I'm going to frame my remarks against the Purdue architecture because I think that'll help me bring out a few points. First of all, I see.  Increasing.  The increasing migration of of IT type technology down from let's say level 4 into 3 and two so.  Increasingly, you see Windows based platforms being used for HM is and.  Engineering workstations, et cetera, it's becoming much more standardised stuff than network. Technology is much more standardised, so the types of switches.  And and so on and so forth. And I think the the real territory for. | | |
|  |  |
|  |  | P11 |  | Operational technology in the CNI remains in the level sort of 1 and 0 area, but that's where a lot of the smart sensors are coming in. Smart sensors and actuators. And so you could regard that as being IoT. | | |
|  |  | P17 |  | Yeah, so I currently lead up complete cyber at the moment my my sort of trade in type role if that was to be given a thing is it's a security architect as how a voice sort of branded myself.  So complete cyber we are well, we work, we are and we still are a professional services consultancy. So we work in both sort of it domains where we're quite a practical kind of company, very hands on in that sense. So very much fixing and remediating.  The problems that we talk about, basically we all talk about risk and we talk about those gaps. If we don't do anything about it quite often the other side of that coin is not, not many people get to see the physical, you know, how do you reconfigure an operating system to defend itself from an attack or, you know, that kind of stuff.  So we do quite a lot of practical side of things, security testing and and remediation engineering that kind of stuff, architecture reviews. So very much you know someone's going to go from A to B.  And they're not sure why they know how to build a solution about how to get from A to B, but they're not necessarily sure about how how to implement those security controls and how that's going to reshape the design. So again, that's sort of my area in, in expertise. So we do that in the IT side. The OT side is a bit more kind of traditional consultancy as I call it, very much kind of advisory risk audit and compliance with a little bit of security testing sort of thrown in there. We've just we received some funding last year to basically go on a sort of.  Product development spree.  I say a spree. It's not really a spree. It's it's one product. But we're trying to sort of branch out a few forks from it, which is an OT security posture scanner.  And the idea behind that is it's a mobile based scanner, it's 4G enabled. So it's using IoT tech because it's it's low cost but has high functionality because of computational memory aspects of it. And we're trying to sort of build a kind of continuous scanning mechanism that's actually done discretely but can be done by the OT. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 138 of 316 |  |
|  | | | | | | |
|  |  | P17 |  | Operators and owners, as opposed to, you know, have a discrete test done by an external consultancy like us or by an external testing company. So we're trying to sort of bridge that gap a little bit and and try and sort of we've actually sort of tried to term the word asset reliability because OT typically sits in engineering and everyone's tried and still will, will still say, look, cyber risks is a bigger problem now than it is yesterday and will be tomorrow.  And I think people are sort of aware of it, but I think the problem is is not necessarily, I think if people hear it too much, the the kind of actual need for it doesn't necessary sink in too much as well as the well as the understanding. So what we're trying to do is coin the phrase slightly differently. And when I talk to engineering companies, which is where a lot of OT sits and tends to be operated by engineering companies or whatever.  If I talk to them about asset reliability, they understand obsolescence management. They understand about component degradation, they understand about maintenance, inspection and intervention. So if I talk to them on those terms, but with a cyber lens on there. So if you inconfigure something insecure.  By your your maintenance, then you might reduce the performance of that asset and hence you know the overall system's gonna degrade or if you expose your system in such a way that it is prone to being attacked, then the degradation factor of that system is also likely to be you know and again it's impacting the asset performance. So we're trying to sort of build something that's coined in that term a little bit so people understand it a little bit better because our awareness is that the maturity levels between OT and traditional IT security is about 30 years in our head. I mean that's. | | |
|  |  |
|  |  |
|  |  |
|  |  | P17 |  | I think we've we've the increase in like you're saying sort of you I don't know whether it's a linear kind of curve at the moment and whether that sort of starts to turn into this sort of exponential rise in in five to 10 years time. But with the amount of computational elements that we're starting to now. So this this is the itot convergence and and realistically we should start to say I TOT and IoT convergence really we should add the IT in there because that's going to fuel it. I think there's going to be a sort of blurred line between.  Because because at the moment the problem we have in industry is there's a real lack of understanding of what assets we have.  How to connect it? How to talk to each other? You know, it's kind of leave the system is is these OT systems typically have a life cycle of 30 to plus 60 years in some cases.  So, and they do tend to stay quite fragile and static in that time period. There will be minor changes. There might be a mid asset life upgrade on that system. So because of those time scales and because of you know, just actually by us humans, you know changes, employment skills, you know lots of information.  Commercial aspects. The information about those systems tends to get lost, and it it there's a lack of understanding and because they don't have the tools or the necessary process to look into those systems, they don't really understand them as well. So I think as you start to increase that footprint slightly, that's going to cause a much wider attack surface. That's the way I that's what kind of worries me at the moment. And whilst we do have frameworks in place, I feel like.  Maybe I'm being I'm going to be a bit biassed here because I'm going to talk from a UK perspective, a UK perspective.  Necessarily from AUSA and an AU perspective, but the kind of enforcement of regulation is probably a little bit more lacklustre than it should be, whereas in the EU you've got enhancements in these D2 you've got the Cybersecurity Act, you've got movements in AI, for example, and and aspects around data privacy as well. So I think I'm not saying they're right or wrong, how they've progressed in, but I think the fact that there's a lack of enforcement and therefore, you know, people aren't going to pay money. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  | P17 |  | To protect their systems, if it's not considered a big enough risk.  So then when you sort of coupled up with a slightly expanded system, I think that's what causes me to kind of be more worried is that we're going to have more.  More gaps in our systems, wider attack surface and then you to finally sort of complement that I guess. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 139 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Just Standard Mitigations as Now** |  | | | | | |
|
|  |  | P18 |  | Within the way we look at functional safety, so when we when we're functional safety. So when we do functional safety, we say.  This is important function that's delivered by this by this system. If that goes wrong, how do we protect the consequence of that? How? What's so? You put protection around it. So you know that it's it's doing something outside its normal operating envelope you have.  Systems that detect that and and do something as a consequence of that to to reduce the impact of that.  Miss operation. So in the a lot of a lot of these.  New technologies new I think they can be deployed safely so long as good engineering practise is done.  And that that, you know for for my area, that's functional safety. | | |
|  |  |
|  |  | P18 |  | if you take AI and you think of AI somehow influencing people to choose one tariff over another tariff, which I don't think is what you're looking at.  That's really difficult to detect and really difficult to do something about it. It becomes a societal issue, not an engineering issue, and that's that's hard to address. But in engineering space and I do think it, I do think it's scopeable and.  Achievable to get protection by and large by good engineering. | | |
|  |  | P23 |  | so for the foreseeable future, it's the cheap attacks and the cheap attack.  Umm, it's still fishing and so the the, the, the kind of the remediations that we need to do in the near future include things like multi factor authentication and what I see like in defense contractors is they do a lot of domain whitelisting and blacklisting. | | |
|  |  | P23 |  | the governments will love quantum attacks, but they'll be they are still I think more than a decade away and and in the meantime, umm, accidents, poor implementation, fishing.  It's going to be what gets us. | | |
|  | | | | | | |
| **Knowledge sustainability across Time** |  | | | | | |
|
|  |  | P15 |  | Better having a better understanding of how previous risks have manifested themselves and and learning what other people have already learnt. We do a lot of relearning what we already somebody already knew, but then they left the organisation. So there's a lot of sort of epistemic like knowledge loss about things.  And therefore like if there's a big churn of people who are constantly circulating around, then that doesn't necessarily stay within one organisation and therefore their organisational ability to respond as it's gone because that's it's with Bob and he's been here for 20 years.  So again, I don't think I've answered your question very well.  Can you remind me what it is again please? | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 140 of 316 |  |
|  | | | | | | |
|  |  | P4 |  | When the problems that I had at the time is that people didn't understand where software came from.  So you know you're you're you're trying to sell them something to do sort of design, but they don't see the problem.  All they see is the malware.  All they see the the big, big figures. | | |
|  |  | P4 |  | But if it's something that the at a low technology readiness and people are trying to just pull that thing up, the higher up the tech redness stack you go, the more people have to understand how it works and the more you have to appreciate the knowledge that people had, I mean, thinking back to, I nearly said IQ, but what was it, the commercialization stuff I did the and you did as well. | | |
|  |  | P4 |  | So there is a yeah.  So if that knowledge is the, so that ecosystem needs to be there.  Uh, and the any technology?  If it's gonna become, if it's gonna be successful, then he's be any, any ecosystem around it.  But that ecosystem assumes an apriori level of knowledge, and sometimes to get that into shape, that ecosystem, you have to find a way of transferring that an appropriate level of knowledge to people as well. | | |
|  |  |
|  |  | P4 |  | And that's not not so much knowledge.  Exchange University to company to company and between companies.  It's knowledge exchange longitudinally through the generations of works, yes. | | |
|  |  | P4 |  | So during you remember Rosetta, this is the aircraft that dropped the Lander on the on the on the sort of comet and yeah, so I was involved with that.  But when it was gonna be something else, when it was gonna be a different commit, and then they had launch problems.  But back at the outset of that mission, it's the only mission I've ever come across where people were thinking about the idea that this is gonna be effectively nearly at 20 year mission and people were gonna retire. | | |
|  |  |
|  |  | P4 |  | And how were they going to manage knowledge for a 20 year, 20 year, 20 year year the your your time the time period because half half of the life of of that of that half of the life of of that of that mission there was no contact with the spacecraft because if you know much about how this stuff works, I mean the comet is coming in from over there.  The spacecraft is there, but in order for the two things to rendezvous, the spacecraft is going to be at the same velocity.  And how do you get that velocity? | | |
|  |  |
|  |  | P4 |  | But what I would say is that I would is that it was what I've said to other people as well, if and what and I said this week I'll see as well is that we do know.  It it's not a unique problem to higher education, there is stuff that can be done to help.  We do know friendly primes.  We are looking at how we can feed the outputs from one project into other projects.  So there are things that we can do to help, but that Will's gonna be there.  It's not my job in government to tell you this is what you're gonna teach. | | |
|  |  |
|  |  | P4 |  | That hardware is going to become obsolete, usually with space missions.  Now it's all done on on an ad hoc basis, or at least it was in my time because Mars Express, you know, it's gonna be 3 year mission now.  It always gets extended because there's a little bit more.  There's a little bit more sort of battery.  We found a little bit more funding, but it's all it's always done on, on the on all this premise on the basis that we might just lose contact and everything will basically finish, but it's certainly with the other project I'm involved with at the moment with this mod development pipeline, we're gonna one of the requirements we've actually put in is this is gonna have to run for several decades.  And how are you going to make sure that that knowledge is sustained over that period? | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 141 of 316 |  |
|  | | | | | | |
|  |  | P4 |  | You basically swing around different planets and different bodies, but a large part of it it was literally in the middle of the solar system, flook close to sort of nothing.  There was still thinking of of knowledge management.  There's gonna be a fight A5 year period.  Nothing happens and then after five period on a set day, they crossed their fingers and send a signal and fortunately things worked.  The thing the thing thing woke up.  But you know this, we're not just talking about Star Trek Into 20 year mission of stuff.  These are people were thinking about this person's gonna retire.  That mission system is gonna have to be upgraded. | | |
|  |  |
|  |  | P4 |  | In in, in in well in, in in general?  Well, it's actually all of that is between teams, across teams, across the supply base.  From you know, if you've got a new technology, you know if all you've got something that the, the that's novel, how do we make sure that everyone knows this?  You know, how are you gonna get that into the curriculum or the professional curriculum?  How are you going to certify people? | | |
|  |  |
|  |  | P8 |  | How to report something went wrong? How to follow up? How to make sure there's something done about it? Now training might be part of those solutions, but if the process is not in there.  For me to A to look if there is something going on when I notice something going on, if you don't give me a way of form to report it to note it down and then to follow up, I think the process is #1.  Training when the other thing when I see usability and so on. All I'm trying to say is the intuitiveness of the so any solution is sustainable if this, if the system is is.  Usable. This is sustainable solution if the processes are in place for me to notice, to get trained and everything. If it is part of the process is sustainable, we can follow up. One of training is not if it makes it so, yes, yeah. | | |
|  |  |
|  |  | P8 |  | Where is it? Where you say people? You mean the users, isn't it? You don't talk about engineers, the users. OK, so, so the training is only one part of the story. So the so the people are not all trained this trip. However, the training is only one part of the story and it may not always be beneficial. The reason being because we get trained on one thing and the thing changes later on or we get trained in one thing.  Forget about it next month. So in terms of sustainability of the training is the problem. So therefore I cannot really provide the training as either A cause or a solution. So the so basically it is a part of the problem, but it is just a part of the problem. People put a lot of emphasis on it, but to be perfect owners, I think the processes are a bit missing in this game. Like if you are talking about, let's say nuclear reactor, different industries and so on, they should be a proper process.  In terms of how to notify like how to notice something went wrong? | | |
|  |  |
|  | | | | | | |
| **Lack of Enforcement of Regulation** |  | | | | | |
|
|  |  | P17 |  | To protect their systems, if it's not considered a big enough risk.  So then when you sort of coupled up with a slightly expanded system, I think that's what causes me to kind of be more worried is that we're going to have more.  More gaps in our systems, wider attack surface and then you to finally sort of complement that I guess. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 142 of 316 |  |
|  | | | | | | |
|  |  | P17 |  | Maybe I'm being I'm going to be a bit biassed here because I'm going to talk from a UK perspective, a UK perspective.  Necessarily from AUSA and an AU perspective, but the kind of enforcement of regulation is probably a little bit more lacklustre than it should be, whereas in the EU you've got enhancements in these D2 you've got the Cybersecurity Act, you've got movements in AI, for example, and and aspects around data privacy as well. So I think I'm not saying they're right or wrong, how they've progressed in, but I think the fact that there's a lack of enforcement and therefore, you know, people aren't going to pay money. | | |
|  |  |
|  | | | | | | |
| **Law on Responsibility Unfit** |  | | | | | |
|
|  |  | P20 |  | who do you hold hold to account for? Accidents involving AI? Is it the user? Is it the developer? Where, who? Who ultimately holds the risk the responsibility for when things goes go wrong? And I don't think there are clear answers to that.  Internationally.  In terms of our domestic regulatory environments, I think that that's a very muddy field again. | | |
|  |  | P23 |  | If you read the studies of the 737 Max.  Yeah, I think about other software accidents.  All the Tesla accidents too.  I'm the there is a kind of thing that happens where the system designer blames the operator.  The operator blames the system designer and it's very expensive to figure out what happened. | | |
|  |  |
|  |  | P23 |  | Yeah, it's it's really big and and this is the reason why, like if Microsoft Word crashes and you lose all your work, too bad for you. | | |
|  |  | P23 |  | But if it were part of a physical product, you might be able to say this product was defective.  You owe me my work. | | |
|  |  | P23 |  | We don't have a regime for dealing with pure software software, untied software tied to services rather than products. | | |
|  |  | P23 |  | so just purely legal side, one of the goals that we haven't been able to quite reach yet is the idea of resilience.  So, umm, the colonial pipeline attack in the US is a great example where.  Colonial actually could operate its pipeline, but they shut it off because they couldn't bill.  And so, like, people froze. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 143 of 316 |  |
|  | | | | | | |
|  |  | P23 |  | we still haven't figured this out of how to kind of get this balance right. | | |
|  |  | P23 |  | any publicly traded company has to disclose material security events.  It's kind the problem is, is that material, umm, a company can make an argument that even losing $10 million is immaterial or even 100, right?  If if you're apple and someone steals $100 million from you.  Like you're like, literally a $2 trillion entity. | | |
|  |  | P23 |  | So that's another that's among the legal the areas, but if it's very complex to figure it out because you don't want to harm innovation and the different people who are writing good code that might be reused in ways that make it unreliable.  So it's a real tough nut. | | |
|  |  | P23 |  | And then when you figure out what happened, you see they're kind of both at fault and you have to make normative decisions about who should be responsible for what.  And and the these are these aren't easy to solve it. | | |
|  |  | P23 |  | I think there's a clear in the literature there's a clear understanding that we need to do systems approaches.  But the law doesn't always require a systems approach.  Evaluation of human in the loop machine interaction. | | |
|  |  | P23 |  | The the current debate we're having in the US will one of the debates is although I don't think it's gonna go anywhere, is whether there should be some type of liability for software mistakes and currently.  In the US, there's broad exemption from tort liability and other forms of liability.  In the UK, excuse me, in in Europe this is not the case.  There's actually more scope for liability, and I'm I don't like Tesla's think they're not gonna get away with that for Long,.  Eventually, a jury will look at that and be like no, like that's.  Umm, so there is that and and.  But the reason why is that Tesla is a product.  So we have a products liability regime for dealing with the software and a Tesla. | | |
|  |  |
|  |  | P6 |  | So in Europe, we are answering now with increasing regulation and laws like NIST two and the Resilience Act. I think I believe it's a, it's a huge burden on the manufacturers and suppliers.  But I believe it's necessary that it's done, otherwise we will end up in a big mess. But nevertheless the question is, are we able to manage it? I mean, just having a regulation or law is something, but you have to enforce it, you have to.  The manufacturers to be able to implement it, we do not have laws that somebody's paying fines. We have lost the system's become more safe and more secure. So the question is, do we have the know how the people, the tools to build the system even we have laws out there to put the system much more resilient. And I would say I said before as a summary when it's even a management summary that we have from infrastructure to communication this data level now. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 144 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Legacy systems** |  | | | | | |
|
|  |  | P11 |  | Oh well, since you are from the software background, I would share with you a completely different concern. I'll change tack completely. I think it's the way that we write software is a concern to me. It's.  I saw an article in the IEEE which I haven't read, but really resonated it said. Is this the year that we did finally deal with bloatware?  What it's talking about, I think, is the tendency to. | | |
|  |  | P11 |  | Right. And then they can continue to work with new software platforms or new new platforms, better, better, better infrastructure, yeah. | | |
|  |  | P11 |  | No, I think what will actually happen is that there will be a a fad for virtualization.  In the same in the same way, but different in that middleware.  Allowed all of the cobalt systems to remain in in stasis because they were understood and proven there'll be something about somehow managing to capture the existing control systems and virtualise them. | | |
|  |  | P11 |  | Yes. Now it's interesting. You talk about impedance matching I it reminds me of the the craze for middleware which took place in the banking sector maybe 20 years ago. | | |
|  |  | P11 |  | And then you'll have all the impedance matching of of the old systems with the new control and all of the problems that has presumably as well. | | |
|  |  | P13 |  | So there have been incidents where.  NHS systems have been attacked and, for example, medical record systems have been subject to ransomware. And while it's inconvenient, I mean.  Somehow the system keeps managing to work.  Reversing to older technologies.  So there is that. But I mean I suppose.  Increasing reliance on those kinds of technologies makes us more vulnerable to critical incidents involving them. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 145 of 316 |  |
|  | | | | | | |
|  |  | P20 |  | So you have those sorts of arguments that are framed in geopolitical terms, and they're about the emergence of, you know.  Sort of arms race dynamics, if you like, around AI software.  In terms of.  Software development for critical infrastructure. I don't know a huge amount about it, but historically it appears to be riddled with vulnerabilities and weaknesses in terms of if you look at the state of secure software in those sectors.  Not a lot of protection around lots of industrial control systems. Wanna cry virus spreading globally affecting the NHS, systems that are still running Windows XP.  Legacy software not being able to update it being used globally, which of course creates a whole new, you know, levels of vulnerability.  Yeah, I mean, I I just think it's a, it's a market which.  Is pretty pretty weak still in terms of security, I I I attempt during the pandemic they had the Aspen Cybersecurity Summit, which is one of these big American events. And Alex Stamos was there, who I'm sure you're you're aware of. And he he said something which stuck in my mind, which was that. | | |
|  |  |
|  |  |
|  |  | P22 |  | Well, it's it's connectivity.  But the the.  No, I can't use the phrase in the wood part, but the the lurking danger that xxx always brings out is that so much critical national infrastructure is built has legacy systems in and they were built to certain standards in terms of, you know, data checking at the front end. And you know now they're being bolted on with lots of add-ons that are brought in from all over the place.  A lot of those systems do not have the same extent of verification of data quality at the front end, and that in fact is the source of a lot of cyber attacks that you know the data checking at the front end isn't happening. And you know there are components built into all sorts of devices that are used in critical national infrastructure that have known vulnerabilities that have been.  In the software.  Incorporates into 260 manufacturers, devices and are now 20 years old and are still there, so there are lots of devices with built in known vulnerabilities, but you know it's not a priority to sort of pull them out because they're working OK, hence the need for AI to record and analyse transient almost failures.  Because we know that there are these buggy devices, these vulnerable devices, these faulty devices in there operating, you know almost 100% but not quite.  And also subject to cyber attacks, because you know, if you've got good enough defences at the front end, the cyber, the, you know, malignant attacks. Sorry, I'm. | | |
|  |  |
|  |  |
|  |  |
|  |  | P23 |  | There's like there are very very basic things like her.  Have you can have you allowed your control infrastructure to be connected to an Internet?  Resource like the most basic A that are not fully ironed out and the attacks against these infrastructures tend to be really basic stuff, not quantum stuff.  I'm gonna find you on LinkedIn and I'm gonna send you an email and ask you to log into the control site or the other.  So it it we really are at at our infancy and and and one of the questions, one of the great questions out there is why why haven't we had a disaster?  Umm the and there is some speculation, you know, like why haven't we had a dam loose control and kill 1000 people and the there is speculation that in fact many of these institutions do not but the you know the larger ones have not connected their control to the Internet and and so on yeah another reason is that many of the infrastructures are quite old and that and the way makes them difficult to attack because no one knows I mean I mean I know Web programming languages but I do not know Fortran and so on. | | |
|  |  |
|  |  |
|  |  | P23 |  | So the needs of the different stakeholders differ a great deal.  There are more and less sophisticated stakeholders.  And I'm sorry that this runs a bit against your that the kind of motivation of your study, but these bodies don't need protection from quantum computers because they're not even ready for basic cyber security. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 146 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Legal - Law** |  | | | | | |
|
|  |  | P23 |  | We don't have a regime for dealing with pure software software, untied software tied to services rather than products. | | |
|  |  | P23 |  | And they also they also have, umm, they they help you get there too, because they want to sell to you.  So they often offer forensic consulting and other kind of advice to get to a lower risk tier.  Umm, so the it's interesting.  The insurance companies, they want this market to work, but they can't figure out how to price it.  So they're in a kind of an interesting area where it's got they wanna make a ton of money, but they can't.  It can't be so high risk that they that they can't pay. | | |
|  |  |
|  |  | P23 |  | The the current debate we're having in the US will one of the debates is although I don't think it's gonna go anywhere, is whether there should be some type of liability for software mistakes and currently.  In the US, there's broad exemption from tort liability and other forms of liability.  In the UK, excuse me, in in Europe this is not the case.  There's actually more scope for liability, and I'm I don't like Tesla's think they're not gonna get away with that for Long,.  Eventually, a jury will look at that and be like no, like that's.  Umm, so there is that and and.  But the reason why is that Tesla is a product.  So we have a products liability regime for dealing with the software and a Tesla. | | |
|  |  |
|  |  | P23 |  | Yeah, it's it's really big and and this is the reason why, like if Microsoft Word crashes and you lose all your work, too bad for you. | | |
|  |  | P23 |  | Yeah, there there's a book written by Josephine Wolf.  She uh studied it pretty carefully.  And the yeah, the premiums went up by like, a factor of 6 in the last year.  I'm but the kind of shadow regulation there is to even get that policy you have to show the insurer that you're doing something on cybersecurity.  And so whatever the insurer says you gotta do.  And so then, in a way of become the kind of insurer, the regular, excuse me. The regulator. | | |
|  |  |
|  |  | P23 |  | So that's another that's among the legal the areas, but if it's very complex to figure it out because you don't want to harm innovation and the different people who are writing good code that might be reused in ways that make it unreliable.  So it's a real tough nut. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 147 of 316 |  |
|  | | | | | | |
|  |  | P23 |  | But if it were part of a physical product, you might be able to say this product was defective.  You owe me my work. | | |
|  |  | P23 |  | But, but changing the law does shape incentives and and so the kind of I think the meta observation is is incentive sick for success and disincentives for externalities and and for harming people.  So that I think that's the kind of the the first issue, right is how to shape incentives and disincentives.  For safety and and for the kind of the things we want, ohm. | | |
|  |  | P24 |  | Like transfer these accountability to the tool, which is not actually accountable for that.  For trying to optimise things, but at the end of the day.  A human perspective and a assessment is always required. | | |
|  |  | P24 |  | Give all the responsibility to them to monitor the operation of a telecoms network or the.  Health of a rich if there's the money turns. If there's a sensors in it doesn't say anything is going wrong, then why should I send someone to do the visual assessment? It's not required. I will have extra cost. Maybe if I do that.  And then the issue is trying to. | | |
|  | | | | | | |
| **Legal and Insurance Framework for CNI in Incidents** |  | | | | | |
|
|  |  | P23 |  | So that I think that's the kind of the the first issue, right is how to shape incentives and disincentives.  For safety and and for the kind of the things we want, ohm. | | |
|  |  | P23 |  | So we need a legal innovation that gets critical infrastructures to the place where, if they can operate, they do and I don't know what that is.  I don't like as far as Colonial pipeline went like, why couldn't they just build people after the fact?  I mean, do you ultimately have meters? | | |
|  |  | P23 |  | And the yeah, the premiums went up by like, a factor of 6 in the last year.  I'm but the kind of shadow regulation there is to even get that policy you have to show the insurer that you're doing something on cybersecurity.  And so whatever the insurer says you gotta do.  And so then, in a way of become the kind of insurer, the regular, excuse me. The regulator | | |
|  |  | P23 |  | You know, if the government says we will pay the bill, keep the power on because we don't want people freezing. I'm the.  So I think we need to legal inner innovation and we haven't found it yet that encourages resilience when there is an attack that can be overcome that that's that's the, that's something I think that's important. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 148 of 316 |  |
|  | | | | | | |
|  |  | P23 |  | And they also they also have, umm, they they help you get there too, because they want to sell to you.  So they often offer forensic consulting and other kind of advice to get to a lower risk tier.  Umm, so the it's interesting.  The insurance companies, they want this market to work, but they can't figure out how to price it.  So they're in a kind of an interesting area where it's got they wanna make a ton of money, but they can't.  It can't be so high risk that they that they can't pay. | | |
|  |  |
|  |  | P23 |  | Or even have the government as insurer. | | |
|  |  | P23 |  | I think another on the legal side. | | |
|  | | | | | | |
| **Long Lived Software** |  | | | | | |
|
|  |  | P17 |  | How to connect it? How to talk to each other? You know, it's kind of leave the system is is these OT systems typically have a life cycle of 30 to plus 60 years in some cases.  So, and they do tend to stay quite fragile and static in that time period. There will be minor changes. There might be a mid asset life upgrade on that system. So because of those time scales and because of you know, just actually by us humans, you know changes, employment skills, you know lots of information.  Commercial aspects. The information about those systems tends to get lost, and it it there's a lack of understanding and because they don't have the tools or the necessary process to look into those systems, they don't really understand them as well. So I think as you start to increase that footprint slightly, that's going to cause a much wider attack surface. That's the way I that's what kind of worries me at the moment. And whilst we do have frameworks in place, I feel like. | | |
|  |  |
|  |  | P22 |  | How is it going to change?  And I was thinking actually it may not. | | |
|  |  | P22 |  | it may not change because of the attitudes of management and the lack of pressure from a regulator and the feeling, you know, I mean, I run a strategy company for 15 years and it was really quite interesting.  The first five years when we were doing board workshop, it was about opportunity. By the last five years, it was all about is it going to hold together for my tenure.  There really had been a change in.  Approach attitude abort.  They no longer were looking for, you know, ways of extending the business. They were willing to defence mode and into how can it go on. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 149 of 316 |  |
|  | | | | | | |
|  |  | P22 |  | I think my view would be that given.  Most infrastructure industries have legacy software that's 40 years old. They're probably slightly guess it's 50 or 60 years old. | | |
|  | | | | | | |
| **Long Term Infiltration** |  | | | | | |
|
|  |  | P20 |  | we're seeing a worrying trend around nuclear security cyber attacks being targeted at nuclear facilities and plants. We've had stories in the UK, as you probably know, in respect of the north of England's nuclear facilities and cyber intrusions into those.  This idea of living off the land seems to be quite prominent, and discourse around cybersecurity. Now, this idea that hackers are, you know, preemptively infiltrating infrastructure and staying.  You know, within those networks with a view to potentially causing damage or exfiltrating value or data at a later time, this idea that the critical national infrastructure you know is is under attack, we don't know, it's under attack, but the hackers are there within the networks and we don't know that they're there and sometimes can be there for a long period of time without us knowing.  So that's a trend that I'm hearing more about now | | |
|  |  |
|  | | | | | | |
| **Magnifying CNI Problems through Social Media** |  | | | | | |
|
|  |  | P15 |  | If you're looking at data to try and understand what's going on in a major incident, I mean back in the day, people would look at Twitter and see what people were saying. If if sort of hypothetically like that that exists in that context. But half of that stuff is misinformation or is about something else or you're using some kind of tool to not like APC going in and looking and saying, oh, I've just seen this, this person's reported this or that person's reported that or.  I know they're analysing the 300 calls that will come into it to make a control room, to understand, OK, what are the key bits of data that we can get from that if those things are being fed by misinformation and disinformation, then that could lead you to.  Deploying the wrong kind of resources in the wrong quantity to the wrong place. They could be at risk.  And therefore you would be delaying. You would either be running the wrong response because you think a different kind of incident is happening. I I you think a firearms incident is happening rather than a bomb.  With with screws and bullets in it that made people look like they had firearms injuries.  It is a firearms instant because my friend's just been shot. They haven't been shot. It was because of the.  Shrapnel and stuff in the in the bomb. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 150 of 316 |  |
|  | | | | | | |
|  |  | P20 |  | One example is this whole new post, Christchurch attack, Christchurch call about eliminating extremism online, which followed the live streaming of the attacks against mosques in Christchurch in New Zealand. And it was like, Oh yeah, you know, sure, we'll have a big lobbying effort to get these companies to remove this kind of information, but, you know.  Has it really changed anything? | | |
|  |  | P6 |  | if we if we use critical infrastructure, that's very yeah, I TITOT systems, power plants, government networks. If you approach them and you just can't can harm the system it can have enormous impact of course a power plant can explode dramatically.  If a gas supply is stopped.  The media is already, I believe, Media's already losing their dominant role and social media. And again, every person is taking over. So if we do a small cyber hack on, I don't know, I'm British petrol and then there is no gas coming out and a few of the stations the same time. I do a big mass social media campaign. | | |
|  |  |
|  |  | P6 |  | That in the UK there is no gas available, people start to go to the gas station, then you have really no gas and then you have to stand still in your country. I would say with to the economic.  Barrier to invest a lot of building a bomb and travelling, but you don't need any kind of investment. Just by fun you can attack big systems. | | |
|  |  | P6 |  | So a classically I would say hybrid called hybrid threat where the the the media domain is combined with with online attack on the certic infrastructure and then you have a mess. | | |
|  |  | P6 |  | All the counter mechanisms are for the moment, not become tricky. Are for the moment even protecting the attackers. Because of course we have to be careful as I don't misunderstand this. I just say it's complex.  But when we want to say we have to free speech, everybody can do it. Yeah, of course. Everybody's doing it. And I have a social media platform where I bought.  Creating 1,000,000.  Votes that this is correct, I'm creating article which are proof in my useless fake news statement and all this stuff and people are less and less sensitive, are reading it believing it and that's what we are doing now in a very call it now in the political system. Yeah. But if we even, which we could we are observing already out in the world if it's controlled and we want to damage your overall system, we can even use the normal population.  To be part of a bigger attack on a system on a critical infrastructure and whatever it is. | | |
|  |  |
|  | | | | | | |
| **Maintenance Not Innovation** |  | | | | | |
|
|  |  | P22 |  | a lot of people are just hunkering down and saying if it happens, it happens. Yeah, we're going to ignore it because there's nothing we can do about it, which is sort of understandable, but.  So for instance.  I can't imagine the forum in which it would be possible to get a discussion going about.  The impact of the attacks on Gaza on individual companies, but there are going to be lots because of changes in the supply chain and but I don't think most companies are thinking that through. They just go if it happens, it happens. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 151 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Malice - intentional** |  | | | | | |
|
|  |  | P12 |  | Major incidents, I mean, yeah, the major incident that always keeps me awake is really sophisticated state backed attack on a content distribution network like Cloudflare optimise. I think you know I I know a lot of people talk about power plants and stuff and water. The thing is with power plants and water they could produce a lot of.  You know unrest. So we saw with the colonial pipeline ransomware incident, you know there wasn't a gas shortage actually there was just a panic that produced the gas shortage.  Or like the ransomware didn't produce a gas shortage directly produced it indirectly. And I think we can expect that from any kind of power plant or or or you know water. The thing is I think that my suspicion is that we may not see a power plant or water kind of attack because I think that that might be seen as this will definitely provoke a military kinetic response, whereas something like a content distribution network, you know, a lot of stuff is going to go down. People's credit cards aren't going to work. And, you know, apparently.  Don't know if you were tracking this, but in Thanksgiving 2023, someone did get into cloud flare via Octa, so we came really close to this kind of EPT attack on the CDN and that would produce, I think that people underestimate how chaotic that would actually be. I mean, yeah, again, you know, you try to swipe your thing at square terminals and point of sale systems and they, you know, they don't work. So I worry a lot about that because I think that they're a great target. I think that it's within the capacity for, you know, AP TS to do.  And I think that it is perceived as not something that's going to provoke a kinetic response. I'm not sure that that's true, but I think it's perceived that way and that really keeps me up at night.  Because that's a world where suddenly I think everyday Americans would be under the impression we're under attack.  And again, this is the US context. I don't know about the UK as much. It's not something I study. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  | P12 |  | Yes | | |
|  |  | P12 |  | Obviously, an apartment attack on Acdn and also you know, I I don't haven't specifically thought about this and because in part just I don't have sources inside this particular well actually I do have a source, maybe I should look more into this but company like square they manage these point of sale systems you know for all sorts of people and there are even point of sale systems out there that appear not to be square point of sale systems but actually rely on square because they they just use square APIs for everything and like you just wouldn't actually be that hard to get inside square and turn it off. You know I can't imagine that they're.  Ready for, you know, a Chinese apartment. It just. And again, maybe they are. OK, maybe they are. You know, maybe maybe cease is in there. Maybe they have former NSA people. But it seems very unlikely to me that that's the case. So yeah, you know, turning these kinds of of payment service providers off like.  I really it seems so easy to do that it seems unlikely that someone at some point won't try it in the next 5 to 10 years. Just be like haha look American capitalism doesn't really work. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 152 of 316 |  |
|  | | | | | | |
|  |  | P12 |  | First of all, so they have a short lived time impact. I think these misconfigurations, but there's scope while they are off can be really big and and I we saw this with Facebook, right, Facebook messed up their BGP configuration and everything. I'm sorry Meta every single meta product was offline. You know Meta's you know like Facebook was offline and Instagram was offline. And I think they even own other other properties that were offline.  And what was so amusing about this to me was that the network that runs their internal systems was also offline, so no one could get there at facebook.com e-mail. And also, you know, they have these systems on their data centres with the badge readers. And those were also networked with the same meta networks. So because of the BGP \*\*\*\* \*\*, they couldn't even badge into the data centre to repair, you know, the thing that was. So what I'm trying to illustrate here is like, although all we've all we've seen are \*\*\*\* \*\*\*.  That were like, just basically misconfigurations, if you know how the network fixed together and you're able to engineer a \*\*\*\* \*\*, you know, like an apt, it can be pretty hard to recover from actually, because if you're saying there's an accidental BGP misconfiguration can make all metapods offer a day, you know, again like a A team of Chinese spies. It was like, has nothing better to do but to figure out how to turn off metapods. You better believe that meta, like all meta products, are going to be offer a while.  You know, like you can really do a lot within the sabotage becomes intentional. And yeah, just these systems are more fragile than we expect. So what would that look like with Cdns with, you know, square? Whatever. Yeah. I mean, these systems could be down for days or weeks even, you know, if they're really, you know, putting intention behind this. | | |
|  |  |
|  |  |
|  |  |
|  |  | P12 |  | But the and what I'm hearing as well is that This is Money. So. So the you're saying the consequence of taking this out is that money would not work for us. So the Internet has become money, you know, for you and I to go down to the gas station and and buy, you know, and buy gas. We need the Internet. | | |
|  |  | P12 |  | That's right, I think.  I think that that's right. I think the financial system's actually really robust. I I I did. So I have in this research spoken people inside the financial system, which is really hard to do because they really don't want to talk to you and they don't want to tell you also how anything works. But I'm actually really convinced like they're table topping. What if the Internet goes down in a way that I don't think tech companies really are or if they are, then it's really, you know, secret even from media people in Cloudflare research don't know about it. If that if they are table topping those things, maybe they just don't know about it, but.  You know, financial institutions really are ready for the Internet to go down and also, you know, look, these financial institutions existed before the Internet.  They know about, they know about not having the Internet and still being able to do financial stuff. The problem that I see with money is that the way that we interact with money has this tack layer, this fintech layer in between. And it appears that we're just doing transactions, but we're actually dealing with Block, Inc or we're dealing with whatever the \*\*\*\*, you know, that that that is interposing themselves between the financial institutions and us and to some extent, the financial institutions have sort of encouraged this because they have this, like, white label system where you can kind of get their white label fight this again, us. OK. I don't know about the UK.  The US these big, you know, settlement banks have these like white label services that they all can compile. You know these APIs or whatever super convenient in the US you can log into any financial institution from any other with Plaid. But what this really means is that there are these like small startups interposing most people's transactions against these financial institutions, which is fine for the financial institutions. When the Internet goes down, their money's all safe and they can be. Don't worry, your money's safe saying this. But from the perspective of someone buying gas at the gas pump.  My money doesn't work. I don't have access to my money. I can't spend any money that causes a freak out. I think so. That. That's. Yeah. And of course, all of those things are now relying on Cloudflare, Akamai.  Exactly. Exactly. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 153 of 316 |  |
|  | | | | | | |
|  |  | P12 |  | But | | |
|  |  | P14 |  | Passed away than ever has been possible before. You suddenly have an attack arena which is vast and with huge numbers of unidentified potential threats in terms of players who can get into that attack arena, you've got some interesting challenges there. | | |
|  |  | P14 |  | On the quantum side, clearly.  Just the massive game changing potential of quantum computing.  Could have extraordinary impact and threat. | | |
|  |  | P14 |  | Which aspects of the of the threat the the only limited issues I can identify around threat is simply that it gives the the ability of I say bad actors and of course.  What we might be talking about is the democratisation of.  Weapons and tools so that bad actors can decrypt.  Encrypted data and get in and penetrate and do weird and wonderful things to the critical national infrastructure. | | |
|  |  | P15 |  | And then afterwards. So I think if you think about technology informing each of those different processes, I think.  There's a lot of opportunity, potentially both to do that badly.  For somebody with malicious intent to try and disrupt the information flow, so either to prevent you from knowing that something something is happening to be creating a risk.  In terms of cyber threats and things like that, but also to disrupt your ability to to collate information, I think there's also just a sort of not even from a malicious intent perspective. | | |
|  |  |
|  |  | P16 |  | So. So I think internally.  Especially with AI for quantum, I think it's way well, no, I'll. I'll talk to Quantum later, but internally for AII think that you know it's it's a it's a dual or technology in the sense that it can be used for attack and of course it has also high utility for defence.  And actually this is the only probably the only response available for defence left. I mean you know the new innovation. So I think it's going to be really.  We're gonna see a lot of uptake uptake and critical infrastructures and the banks are doing it and they've been doing it for a for a while. So they're not, it's not a surprise to them. It's just like still probably very murky in terms of determining which products or services or use cases actually makes sense for them in from a security delivery perspective. So you know is are the new technologies that are being promised to them to enhance their.  Cybersecurity posture gonna be useful, or they're gonna create more work.  And by generating too many false positives and and so on and so forth. So I think that, man, it's gonna be probably.  Major efforts on the parts of critical infrastructures to.  Embed AI technologies into their cybersecurity solutions and. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 154 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | Malicious activities against critical infrastructures.  We've heard about it for 10 or 15 years. As you've read in the report, and some use cases and people used to make predictions, but I think now we are starting to see the adoption of AI technology by attackers to.  Identify vulnerabilities of critical infrastructures, craft pack tools or design some.  Customised messages for victims of spearfishing or fishing attacks. So I think in the near term and I think it's going to be with us for probably in terms of us understanding the risk and how they can be used for risk design and deployment for the next 5 to 10 years AI.  And in Canada, we have A and I'm sure I think you also have that in the UK, but a very strong quantum computing.  Community and I think that if we are looking a bit further in the horizon, I think 10 to 25 years ahead. I think the quantum threat will probably be something that will also be very, very disruptive. And as you know, that's something that we should pay attention right now. But it's so far in the future and so unpredictable.  'Cause no one knows exactly when someone is gonna be able to.  To harness quantum computing to break all the all the encryption. So it's very for companies that are facing on a daily basis the constant barrage of conventional cyberattacks and then now AI powered cyberattacks. The quantum threat is like something that just doesn't register because they just have no bandwidth left. | | |
|  |  |
|  |  |
|  |  | P16 |  | Well, it's it. Well, it's it's a it's it's a very I mean it's not. I'm not claiming it's something very complicated. It's just like the fact that when you have those interconnected interdependent systems and you have like a very autonomous tools now being developed to attack or to defend. So you have machines that are making decision just like in the stock market when you have an initial, you know, a tiny event.  Generating a cascade of decisions.  Decisions by, you know, in microseconds by.  Software that is trying to beat the crowd. So I think that's why we're probably going to see when when AI is going to be manning a lot of our cyber defence systems and AI are going to also attack and are going to let loose by malicious actors to attack certain targets. It's very possible that.  You know, they didn't think of all the implications and the the attack might get out of hands and and and keep on propagating outside of the initial bounds of what was planned or envisaged. And we end up with, I think the.  What's the? What's the attack that you know what? There. What's what's happened with the Russian malware?  Can't remember one. I cried, so not pity. I wanna cry 2 pieces of malware that were supposed to be contained to attacking Ukrainian.  Organisations. But because of the the fact that a lot of Western companies had outposts in Ukraine were operating in the Ukraine, then it was used. | | |
|  |  |
|  |  |
|  |  | P20 |  | So I guess I'm I I guess I'm worried in about an interested in the intersection of cyber attacks, manipulation, subversion and the use of AI in ways that affect the healthy running of our democratic systems and processes.  And again, you know that there are definitions of critical infrastructure which include our electoral systems. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 155 of 316 |  |
|  | | | | | | |
|  |  | P20 |  | Yeah, there's the you know, obviously if you if you spread misinformation and disinformation, you're kind of injecting bias into the world, aren't you? But I mean they I guess at least I've thought about them as separate issues. Yeah. I mean, look, I think that technology means that we're becoming ever more capable at at developing and disseminating disinformation deliberate, deliberately spread, spread misinformation, misinformation.  And that people are absorbing a lot of misinformation, which.  You know, might not be spread deliberately, but which is just out there.  So I think the capabilities to do that are are becoming more sophisticated.  Obviously we're trying to regulate that, but it's difficult because it means rely on being reliant on.  The companies where the disinformation is spreading.  So that's Twitter or Facebook or Tiktok, and we don't have regulatory control to sufficient degree of those companies. Companies, in my view. One example is this whole new post, Christchurch attack, Christchurch call about eliminating extremism online, which followed the live streaming of the attacks against mosques in Christchurch in New Zealand. And it was like, Oh yeah, you know, sure, we'll have a big lobbying effort to get these companies to remove this kind of information, but, you know.  Has it really changed anything? | | |
|  |  |
|  |  |
|  |  | P20 |  | There's just as much violence and and misinformation and disinformation and extremism online as there is there ever was probably, in my view, I don't know whether I'm statistically accurate in saying that, but it certainly seems that way. So yeah, I think the trend is in a bad direction. And in terms of data bias and integrity, I think that that's a big problem. I'm one of the things I'm doing at the moment on the AI security stuff, is looking at data poisoning as a method for, for manipulation.  Predation of of AI and algorithmic systems and and the data they're using. It seems to me a pretty.  Prevalent form of malign activity, one that's growing in sophistication.  I think I've been sceptical about this idea that you can ever have completely unbiased data sets, but data reflects the bias that's in society.  But it can also be very consciously manipulated by malign actors in ways that will lead AI to not function in the way that's intended intended to so.  I think I'm interested in.  You know, it's a disinformation side also the the.  The growing sophistication of data poisoning, interference with the integrity of data. | | |
|  |  |
|  |  |
|  |  | P21 |  | To current event not decrypting, they are they're currently, they're not decrypting, they're encrypting, if anything. | | |
|  |  | P21 |  | A very difficult to quantify out, no, I don't think that's that. It's a bit coming up with something that's previously unheard of. I think it's just the the scale and scope might change, yeah. | | |
|  |  | P21 |  | And the focus, as I said right now, criminals can still make money easily elsewhere, so. | | |
|  |  | P21 |  | But or just leaking or exfoliating in the last place. But one could imagine a scenario where this, perhaps less on a criminal spectrum, more in an espionage spectrum where they're harvesting data that is encrypted.  They currently can't access, but in retrospect they might be able to access that by 2040 because by then they have the capability to decrypt. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 156 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | OK. But so so you see the stolen data and analysis of that with the aid of AI as being potentially something really quite.  You know, quite worrying. | | |
|  |  | P21 |  | Yeah, I think there is a lot, a lot more data out there than we currently assume. This is by the darknet, but also commercially available data. I think it's quite.  Daunting at times, how much data is out there? We don't. We don't quite grasp, but particularly how much information that data.  Turns into if you overlap certain data sets.  And I think that our ability to really.  Use. The data will increase because at some point it will be more about the quality of the data rather than the quantity, and I suspect there may forthcoming technologies will enable us to to sort of make use of equality alternative to something qualitative rather than just relying on on everything that's publicly out there right now. | | |
|  |  |
|  |  | P21 |  | So I think you can turn what we'd sort of now think of as more of an indirect victim. So not the past, who's actually suffered the ransomware attack by the person who whose data has been leaked. And all of us by now will have gotten emails from capital. I don't know whom, that our pension date has for leaders of health. I think it could could expand the notion of who's a victim. And then in turn, those who've previously been indirect victims, they could be turned to direct victims because they might then face crime fraud or something else.  As a result. So that would mean psychological, financial, reputational harm on them again. So it's really expands the the notion of who can be a victim. | | |
|  |  |
|  |  | P21 |  | Yeah. So the one of the other papers that we published on this was on the the harms that result as a consequence of ransomware attack. And this is ransomware, but it could also be other encryption or intrusion based crime. So it could be broader than that.  And in our research, there was no indication that some of the data that's been harvested by cyber criminals and leaked on the dark net, there's.  Additional harm resulting as a consequence of that because.  Criminals might use that data for further criminal activities.  The fear is that if I'm a lawyer, I've suffered from lansomer attack and my my clients data has put on the dark net. They are then exorted and they become subject to further crime because of that.  In our research, there hasn't been evidence for any systematic exploitation of that data, primarily because cyber criminals don't have to, because they're money driven, they have easier ways to make money. It doesn't have to be that complicated.  And there's that amount of data that they harvest is also it will change. I think with AI and better and more computing and passive.  Do you? But it's quite an effort to sort that data to analyse that data to then turn it into something that you can use for further crime, right? So that amount of effort and storing that data in the 1st place and you have to pay for that and so on and so forth. Yeah, that is currently not being exploited to the extent that one might fear. But I think that is something that could very much change if there's different data analysis capabilities. | | |
|  |  |
|  |  |
|  |  |
|  |  | P21 |  | But I mean, you can also can also be less sophisticated, right? I mean, a lot of what we're seeing in this context isn't actually as sophisticated as as something like that. But by 2040, who knows? I mean, cyber criminals have been pretty inventive and pretty have welcomed new technologies with open arms to ensure that the business remains lucrative. | | |
|  |  | P21 |  | Or perhaps also the ability to, in retrospect, in retrospect, decrypt some of the data that's been harvested. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 157 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | Extortion, some ransom and theory assumes that you encrypt something, but you gross just blackmail without encrypting something. Just say, OK, I'm threatening to leak that data.  But I also think.  Industrial espionage, perhaps. | | |
|  |  | P5 |  | You know, they're very localized.  Usually that don't propagate out somewhere because they catch it right away.  Somebody does, and so they correct it, but a malicious intent is far different than that.  They have campaigns that go to all kinds of things towards the end goal, whatever it is that they're wanting.  And so that's why typically we focus more on the malicious side of things and not just the random mistakes. | | |
|  |  |
|  |  | P5 |  | I I have nothing to prove this at all, but I'm guessing just from my experience that I've seen over many, many years that the incidental mistakes that people make type in the wrong whatever doesn't typically lend itself to catastrophic failures or consequences. | | |
|  |  | P5 |  | But but yeah, yeah, that's that's a very as I suppose there's an element of mistakes are kind of random, so whereas malice is not, it will, you know, push everything in the same direction. | | |
|  |  | P5 |  | How | | |
|  |  | P5 |  | So the question I think implies what would the goals be of the adversary?  So that's the very first thing you have to ask, because what are they trying to do?  And then what do? | | |
|  |  | P5 |  | And so again, our our biggest things that we typically do is this sabotage and theft type.  And by the way, the theft part are usually blended attacks because you know cyber can't just mysteriously grab with the bits and bytes and pull material away. | | |
|  |  | P5 |  | Yeah, but you can certainly disable physical protection devices, cameras, card readers, things and allow a person to get into steal that stuff. | | |
|  |  | P5 |  | That yes, there is a determination to get through all those security barriers that we put in place. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 158 of 316 |  |
|  | | | | | | |
|  |  | P8 |  | If my people, if I measure something like this around this, isn't it? So it's more like it's very difficult to distinguish between a fault in the system and a malicious like an attack. So a lot of people, I don't think we are really trained, we can really distinguish the difference between what went wrong and why it went. So we may understand what happened. Like 2 cars are crashed in terms of why that happened. I personally believe.  We will not be able to be able to say that unless we really trained and we actually know what to look for.  Some people we know it very well because they know what to look for, like some of them are like an experts here. We are trained partially for that but is much like in every job. No, no. It's really very hard to know. Yeah. And this might be, yeah. | | |
|  |  |
|  | | | | | | |
| **Mass replicated attacks from monoculture software** |  | | | | | |
|
|  |  | P10 |  | We the the the risk of monoculture in security subsecurity in particular is if everyone, let's say, everything government is run on Microsoft because they're very good and you know, I've no criticism of Microsoft. But if it's a monoculture, you get one floor. Great, you've got one floor and it gets, you know, it kind of goes across the piece and there's again just looking at good data. Microsoft, if you if I am a malicious person and I want to you know create a but I'm I'm going to target Microsoft because it is.  It it is buggy and it's going to have, I'm going to get my greatest bang for my buck. I'm not going to be trying to work on something. What is it that submarines run on? You know something that's really archaic, you know? That that's that's less. That's less of a challenge. So those sorts of things. I think that that monoculture in in, in technology and cybersecurity is is a real issue. | | |
|  |  |
|  |  | P16 |  | You know the the the, the system replicated and just kind of.  Went a wire and just went all all around the world and paralysed a lot of companies so that that's the idea of propagation. | | |
|  |  | P18 |  | And coming with increased digitization comes.  The difficulty in in getting diversity into into systems. So if you've got.  Have you got analogue systems and digital systems? You know by by design there's an obvious.  Diversity of approach between an analogue system and a digital system. If the if analogue systems no longer become available because of that increased amount of digitization, then you're losing that diversity and you end up. If you're not careful, being susceptible to things like cyber attack across multiple.  Platform. So we intended to be diverse. | | |
|  |  |
|  |  | P6 |  | also for energy, network producers and energy producers, any kind of others, all these.  Alternative producers, I mean the individual windmill is not critical.  But if I have 1000 of it and all of them have the same control software and I do an attack on the control software, then I can control thousands. I can also again attack the whole state so and I believe just because the malicious actor in this critical infrastructure is not yet well understood, well researched, period enough. And that's the reason why the impact is higher. So the threat is higher and it's more critical to look on this than the accident side. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 159 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Military Response Sanctions or Arrests Expected to CNI Attack** |  | | | | | |
|
|  |  | P12 |  | The thing is I think that my suspicion is that we may not see a power plant or water kind of attack because I think that that might be seen as this will definitely provoke a military kinetic response | | |
|  |  | P20 |  | You know, there's obviously the sanctions regime and the thing, you know, that putting putting sanctions in place over malicious cyber activity is another thing that's.  It's important. I mean, I've done a lot of work on cyber diplomacy as well. You know, how can you diplomatic mechanisms to try and improve the security and safety of critical infrastructure? You know, we've got AUN, treaty ongoing at the moment on cyber crime, which I'm sure has provisions about critical infrastructure. | | |
|  |  | P20 |  | about the malicious actors and their behaviour as well, how how can we shape that?  That's the other work I'm doing. It's on Russian and Chinese hackers and and and the motivations that the reasons they're doing what they're doing, the way these countries think about the utility of these sorts of operations targeting CNI, how their behaviour changes, I think we need to do a lot more to understand.  If if I use this term, the culture of these groups and these individuals. | | |
|  |  | P20 |  | It's about encouraging an international normative environment that says it's not OK to target hospitals and civilians civilian infrastructure.  And it, you know, it took a long time with the for the international system to embed those principles through the Geneva Conventions, right? It might well take a long time to embed normative principles in the international system around AI and cyber. But there are people actively working on that. And so, you know, there's room for diplomacy, international negotiation, international prep, pressure, incentives for bad actors to stop doing what they're doing, more punitive measures, sanctions, punishments, retaliatory cyber.  All sorts of things which might try and deter this type type of activity. | | |
|  |  |
|  |  | P23 |  | the US approach under President Obama was to start indicting people and that and people made fun of it.  They were like, well, the Russians are never gonna extradite.  So and so, but in fact we've caught like a bunch of people and it's typically.  Criminals who are going on vacation and they don't know that the FBI is watching them and they go somewhere and the pick them up like we arrested the son of a Russian senator on vacation.  And he's currently in prison for hacking, so part of, yeah, we don't without government participation.  I'm sorry without, you know, with the Russians of the world.  I'm we've had to depend on this kind of human mistake of going on vacations true with Chinese too. | | |
|  |  |
|  |  | P23 |  | We've we've caught several Chinese hackers on vacation. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 160 of 316 |  |
|  | | | | | | |
|  |  | P23 |  | also might be a protecting us as well is the legal notion surrounding acts of war in the sense that if there were an attack that caused, let's say, a major dam to malfunction and it killed hundreds of people, that I think.  Enters the kind of we have been attacked level where the attacking government would have to contemplate being bombed.  And so I think that's another kind of guardrail right that's stops like stupid people from doing things | | |
|  |  |
|  | | | | | | |
| **Mindset** |  | | | | | |
|
|  |  | P18 |  | And then and people motivation rather than rather than, you know, technical motivation and necessarily keeping the lights on, you know, it's it's all about kind of.  Personal motivations as well. Profit, those sort of things fairness. | | |
|  |  | P18 |  | Yeah. So, so when we think about physical things needed to be happening, we also think about procedures around there. And we think about.  Plant people and process so you know those three things in order. You know, an effective system.  Has plans aspects to it. It has the people aspects and it has process aspects to it as well. So so we do think about it in those terms.  Yeah. And the stuff that I'm doing again with offgem, you know, I'm trying to take a systems thinking approach into that. You know, when you're looking at especially on.  You know, I mentioned about kind of the impact of AI on society rather than national infrastructure. You know, that's very much.  A technology and people centred approach.  But then you know, in terms of national critical national infrastructure, you know the the markets can have an influence on that as well. And that's you know that the markets isn't a physical thing. That's that's people. | | |
|  |  |
|  |  |
|  |  | P18 |  | So | | |
|  |  | P18 |  | Including the people. Yeah. Yeah, yeah, yeah. Yeah. So and.  And in yeah, that that to some extent.  Picks up on that interconnectedness, you know, and and and.  Yep. So we've got something really complicated or complex rather, and it's gonna have an impact on something if let's not, let's not just stop there. Let's think about the knock on effects of that. So yes, it's a whole system's view rather than thinking too narrow. Narrow. I mean, there's a limit, isn't it? Because you could end up with everything being the same problem. So. But, you know, thinking beyond the technology I think is important. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 161 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | I think we tend to think too narrow about these things and we tend to focus in on the shiny stuff in the middle, the technology.  I think we have to step out from that and think about whole system.  So if you're going to do something new.  Thinking about the consequences of failure.  And and you know and developing that. So you actually understand.  How the failure of the AI is going to propagate and result in whatever what the risks, you know, the likelihood of those happening, the consequences happening. But that's a whole system's view rather than just looking at the AI we tend we have a tendency to focus just on an AI, for example. But we've got a step away from that and think about the whole system.  And and its potential impact. | | |
|  |  |
|  |  | P18 |  | Yeah. So think about the the likelihood of failure of AI is 1. The likelihood of having a cyber attack is 1, and and if you think if you think about it in those those that those terms, you might seem kind of negative and pessimistic.  But actually it drives the right behaviour and the right engineering and the right kind of protection or whatever.  If you think Anna will be OK, then you think you can guarantee that you're going to get bitten. Yeah, yeah, yeah. | | |
|  |  |
|  |  | P19 |  | And I think that that's important because I think some folks in the past have thought if if we if we build enough protection into systems.  Yeah, well, there.  But they were all right.  But you have to think about what happens when the world gets benefited.  Yes, you have to to think about the perhaps unlikely, but all too frequent penetrating of the cyber war.  What happens when the bad guys get in?  Yes, you've got to be prepared for that.  And that's about. | | |
|  |  |
|  |  | P19 |  | I suppose that critical system would be would be a railways as well.  And yeah, some ways and and of course they're used to thinking of safety to safety is another aspect of this and.  And of course, an organization like the like, the real world, make sure that they have so many safety systems that you you can't have two trains in the same block of line at the same time.  Yes, the signal has to has to work perfectly.  Course it doesn't always.  And what happens if if the driver? | | |
|  |  |
|  |  | P19 |  | and the and the seniors in these organizations were hiding behind this possibility that that you could persuade people that these systems couldn't go wrong or couldn't do something wrong.  Yeah, it's quite remarkable.  Strongly so software is it's not magic, it's it's it's it's, it's logical and people we need to be not frightened of myself, but they need to be trained to know more about it.  So you see, this is an education.  Yeah, absolutely. Yeah.  Yeah, putting in these traditional industries, yes, like process control and utilities that need to be more people and and they're doing this anyway. | | |
|  |  |
|  |  | P19 |  | As as a problem.  Then there's the the dead man's handle.  Is that yeah, familiar remedy for that?  They they have thought of all of these things.  And and the nuclear industry, of course, has got lots of that kind of thinking.  Umm that you don't often get to to design a system like that from scratch and you're asking about how you would go about doing a resilience system.  I think some of the work that I and others have done gives a kind of formula for how you would go about doing the thinking right, right? No.  So I I I I don't know if if you're aware of some of the recent books and Zillions channel. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 162 of 316 |  |
|  | | | | | | |
|  |  | P19 |  | So this is training skills and awareness.  Awareness. Yes, yes. | | |
|  | | | | | | |
| **Multidisciplinary - cyber informed engineering - software resilience engineering** |  | | | | | |
|
|  |  | P11 |  | I mean, one of the solutions I think to the observability and the complexity problem is to make our systems less complex and more observable, but they then cost more money.  Unfortunately, you can't do that additively. | | |
|  |  | P11 |  | As | | |
|  |  | P11 |  | The safety engineers I work with abdicate responsibility, and if you read the safety standards and I'm I'm on a couple of committees and such like and I've reviewed one for railway, another one for nuclear, another one which is general, and they all suffer from the same problem as I see it, the safety standard says line one. Assume the security system is perfect and don't worry about it. | | |
|  |  | P11 |  | It's | | |
|  |  | P11 |  | Well, one of the things that I would do.  Is stop teaching computer security as a separate specialism.  And make engineers and computer computer engineering the words don't fit together. But anyway, making the people who build computer based systems, software, software designers and engineers of other kinds, especially especially systems engineers.  Make them responsible for delivering.  Systems which have a known quantum of resilience. | | |
|  |  |
|  |  | P11 |  | Nine shuttle, yes.  The IT it takes something like that to make people stop and say, well, how did this come? How did we come to this? I actually sent an e-mail to a colleague in NCSC saying something along these lines, like particularly the safety security thing. What causes me real anxiety is that at some point and I'll, I really will have retired by then. There will be the equivalent of the O rings or the OR the the Nimrod scandal.  And people will say.  How did we come to build industrial control systems in this manner?  Didn't we know? | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 163 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | Build it well, actually a better one would be the O rings in the 1980. | | |
|  |  | P11 |  | You could say they're non functional or whatever functional requirement, but putting them in as part of the requirements for the system that you're building.  But I think we just lack the language. I think we lack the awareness.  So people aren't doing it, and and therefore perhaps what does concern me is that we are rushing headlong to build systems.  That at some point in the future we will discover weren't built well enough.  If you look.  You know the history of, for example, safety.  Hat and cave is that the report I'm thinking of, you know about? How did we find ourselves? | | |
|  |  |
|  |  | P15 |  | Is if you look at the technological systems that support emergency services response and interoperability.  There are already challenges when it's working well because you're working with people who aren't necessarily like technically proficient in that way they aren't normally used to doing XY and Z, and this might not be at the forefront and therefore it's a sort of training and exercising and skills fade thing of OK, don't normally have to engage with this system very regularly, and I've forgotten how to use it. And now X has happened and the the plans that they need to do Y and I can't remember how to turn this thing on or I don't have the password like like you would be amazed how much like with the really basic stuff.  Goes wrong.  And therefore I think anything around making, I think there's a potential for.  Comms and information sharing and technical information sharing.  For situational awareness and response and decision and making good quality decisions based on as much information as well, not as much information as possible, can source it possible to get overwhelmed by information, but normally you end up not having enough and then you have too much of it.  And therefore, like there's a, there are opportunities I think for technology and technological advances to.  To aid those processes, but there's also quite a lot of opportunity for unintentional, unintentional errors with those. | | |
|  |  |
|  |  |
|  |  |
|  |  | P18 |  | And then and people motivation rather than rather than, you know, technical motivation and necessarily keeping the lights on, you know, it's it's all about kind of.  Personal motivations as well. Profit, those sort of things fairness. | | |
|  |  | P18 |  | Yep. Gotta be careful, 'cause. That's what I am. Yeah, I am. Yeah. Yeah, I'm a systems. I'm a systems engineer. So. So, yes, I am thinking about systems thinking and. And I'm thinking about it in both the traditional sense of systems thinking. So systems engineering, software engineering, that's sort of approach. But I'm also thinking about it in bringing in those human elements as well. And at Lancaster University, you've got the soft systems methodology that kind of.  Checklist developed, you know, so you know that that sort of thinking where you're you're looking at hard stuff as in physical stuff, but you're also looking at human behaviour around that as well and motivations to do things and and all that sort of thing. So it's not just a like a physical system, it's as you said.  The the kind of interplay of of people around that physical system as well, I think is important. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 164 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | Yep. So would that mean that will result in loss of function, wouldn't it? And and potentially permanent damage within within those systems so that recoverability is important you know.  And in terms of loss of function that goes back to.  What I was saying about functional safety, you know, don't don't put all your eggs in the AI basket.  That's be sensible about it and have a protection that says if AI does this then.  At least put a flag up and say, hang on, you know it's it's suggesting we do something ridiculous here and do something. So I. Yes, I agree with that, that statement. But I think the stuff that we can do well, there's there's approaches that, you know imply that you can recover from it or you can protect against it. | | |
|  |  |
|  |  | P18 |  | So I'm less. I'm less worried about things like AI.  In that in that sense.  In in that application, if you take AI and you think of AI somehow influencing people to choose one tariff over another tariff, which I don't think is what you're looking at.  That's really difficult to detect and really difficult to do something about it. It becomes a societal issue, not an engineering issue, and that's that's hard to address. But in engineering space and I do think it, I do think it's scopeable and.  Achievable to get protection by and large by good engineering. | | |
|  |  |
|  |  | P18 |  | Within the way we look at functional safety, so when we when we're functional safety. So when we do functional safety, we say.  This is important function that's delivered by this by this system. If that goes wrong, how do we protect the consequence of that? How? What's so? You put protection around it. So you know that it's it's doing something outside its normal operating envelope you have.  Systems that detect that and and do something as a consequence of that to to reduce the impact of that.  Miss operation. So in the a lot of a lot of these.  New technologies new I think they can be deployed safely so long as good engineering practise is done.  And that that, you know for for my area, that's functional safety. | | |
|  |  |
|  |  | P18 |  | Yeah. So, so when we think about physical things needed to be happening, we also think about procedures around there. And we think about.  Plant people and process so you know those three things in order. You know, an effective system.  Has plans aspects to it. It has the people aspects and it has process aspects to it as well. So so we do think about it in those terms.  Yeah. And the stuff that I'm doing again with offgem, you know, I'm trying to take a systems thinking approach into that. You know, when you're looking at especially on.  You know, I mentioned about kind of the impact of AI on society rather than national infrastructure. You know, that's very much.  A technology and people centred approach.  But then you know, in terms of national critical national infrastructure, you know the the markets can have an influence on that as well. And that's you know that the markets isn't a physical thing. That's that's people. | | |
|  |  |
|  |  |
|  |  | P19 |  | How how do we?  How do we coped with this?  Given that these systems are not not not that well protected, but the moment Charles, I think that more research is needed in the field to to, to design and and actually to after the fact.  I resilience into systems, could you?  You can't just start again and and and they'll just look from scratch.  So I think it's important to to use people, people from other disciplines to think about the the risks involved in no resilience comes at a cost, because with resilience, we're talking about adding redundant components and paths.  So the the these are are gonna cost and I I suspect that in the past systems and service providers have maybe been a bit reluctant to to add.  Yeah, costly resources like this, of course. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 165 of 316 |  |
|  | | | | | | |
|  |  | P19 |  |  | | |
|  |  |
|  |  | P19 |  | Study hard.  Yes, I I I think that Donald Davis and and and the the work that they brought up in the mid to late 1960s is amazingly forward looking.  I thought it predictions for the need for and the possibilities of data networking and and of course it's no rapidly progressive.  Of course it got picked up a lot in the United States with the vast amounts of money.  They were bought into first, the ARPANET, and then the infinite developments.  Yes, but but the UK and European institutions played their part and fact they played more of a part than this recognized here.  So I'm interested in looking at what the contributions actually where.  I think they deserve a bit more credit than the they currently have. | | |
|  |  |
|  |  | P19 |  | We're talking about the 1960s, but a national physical lab in the UK was one of The Pioneers in in what was called packet switching at the time, and they they come up with a word packet.  They also came up with the word protocol.  Sorry nication systems and and they they particular Donald Davis who was the leader of the group there.  Proposed data networking would be a big thing, a bit need in the future, and the the telephone companies simply refuse to accept that he thought that voice would always dominate.  They just couldn't see the future.  And Charles, this is one of the problems that we've got seeing into the future. | | |
|  |  |
|  |  | P19 |  | So, Charles, that, this, this idea of of your project looking into the future is absolutely right, because we need to think about the the challenges that will come up and the risks that that we have to overcome or at least to take into account. | | |
|  |  | P19 |  | You using Tonkin and machine learning systems?  I don't like using the word.  Terry I but but but some kind of.  Trained systems data process which are quite quite complicated these systems themselves.  I think the introduced more vulnerabilities than than you might imagine, so it's even more important to think about resilience by design.  So I any kind of any kind of system that that could be part of the critical national infrastructure needs to be designed to resilience in mind to think resilience and and in fact some of the stuff that I've written in recent years has been to try and get this message across. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 166 of 316 |  |
|  | | | | | | |
|  |  | P19 |  | Now I I mentioned about RTI and about organizations and people.  Working with people from other disciplines is really important in this because the source of many problems comes not not just from the technology, but actually more from the people.  Yes, if if you if you get side successful cyber taxes, it's often the case that the someones been engineer.  Human engineer.  Yeah, there may be malicious insiders.  They make you will be familiar.  Yes, kind of thing that's upset.  How how do we deal with this? | | |
|  |  |
|  |  | P20 |  | I yeah, probably a bit of a cheesy answer is it's people, it's training.  And creating the the skills in our economy and in our society that have the capability to deal with this stuff.  I think it's possibly changing our political processes so we're less cowed and in Hock to these big powerful technology companies. | | |
|  |  | P20 |  | I think the the security by design trend is a is a good and important one. I'm a bit sceptical about whether it's going to really take hold as I've said, but I mean that's at least it's the right principle in my view. | | |
|  |  | P5 |  | Umm, there was three of us that are around the 2014, 2015 time frame were were sitting in a room together, working on a common project and we were we were just noticing that a lot of engineering firms, a lot of end user utilities operators, cause we were in the critical infrastructure mode at that time.  That everybody that we talked to, especially the engineering people, nobody had a clue about cyber security and that's only what nine or ten years ago, right? | | |
|  |  | P5 |  | And so that's where that cyber informed engineering comes in.  Is that idea that engineers need to fully be aware of cybersecurity?  Not necessarily experts they can call in the experts, but they have to be thinking absolutely and all their designs about cybersecurity. | | |
|  |  | P5 |  | So that's kind of the history of how cyber informed Nigerian came about.  We do talk about in those documents that it's not just engineers, but it's also for Technical Support personnel that should have these ideas and concepts in their heads as well, because you want to maintenance person, to not just plug a USB into their maintenance laptop and then plug into a PLC, right? | | |
|  |  | P5 |  | OK, so that has just a lot of questions about different phases of the systems engineering lifecycle, right of things that an engineer should be thinking about and have good answers for.  And if we we thought if they could answer all of those questions with great answers that you have a high probability that you would have a more secure design than a less secure design.  OK, of course I'm not dealing with absolutes here because you can't do that. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 167 of 316 |  |
|  | | | | | | |
|  |  | P5 |  | Umm, a person by the name of xxx, who was working at the INL for the Department of Energy in the Caesar.  I don't know if you know what Caesar is.  I forget what it stands for, but it's the cyber security portion of Department of Energy and she was able to acquire some funding to take these conceptual concepts into practical implementation.  What would these concepts look like in the practical world so that we could hand something to the engineers in the industry and have them guided through a process right?  That would help get more secure designs and so through the last several years they've come up with a strategy for cyber informed engineering that the government our government signed off on.  And then we've put out Revs.  Zero of what's called an implementation guide.  What this have you seen that yet? | | |
|  |  |
|  |  |
|  |  | P5 |  | The other aspect was how do we reach the current engineers that are in the fleet in industry, you know early year, mid year career you know final career let me how do we reach, how do we reach the old dogs.  Don't wanna learn new tricks, right?  And so that was quite the challenge to us.  And So what we did is we came up with some concepts that we thought would be very important.  That engineer should understand and we wrote an initial conceptual report paper back in 2017 that listed out these fundamental principles that we thought they should be aware of.  And be thinking about it in their designs, their modifications that they perform operations, maintenance, all of that.  So that report came out that was funded by the Department of Energy at the time.  It kind of sat there on the shelf for a few years and then. | | |
|  |  |
|  |  |
|  |  | P5 |  | And so we said ultimately we have to reach the educational institutions and make sure that they start talking about cybersecurity to their engineers.  And once that happens, they come out of school.  They already know, just like safety, I need to consider security.  But typically, engineers again in the US pass never really had that training.  So that was one aspect. | | |
|  |  | P5 |  | So we were we were talking to ourselves.  What is wrong?  What are we missing?  Why is our message not getting out?  OK, so that was the problem statement.  Basically that we were talking the three of us were talking about and collectively we came up with the idea that we thought, you know, engineers are typically not taught in the universities about cybersecurity, at least in the US, not so much. | | |
|  |  |
|  |  | P5 |  | And what's what was more concerning to us is, at least at the Idaho National Laboratory in the early 2000s, you know, 10 years prior to that, we had done all of this national skate, a test bed.  And we had done all these assessments and we talked to the utilities and we talked to the vendors.  We talked to a lot of people in the industry.  In the in the engineer still weren't coming on board, right? | | |
|  |  |
|  |  | P5 |  | In safety as well, correct and and again it comes back to, you know, the adversary needs to understand, especially if they get into the operational technology side of what is the physics behind what they're trying to do.  And back to the Cyber informed engineering.  That's one of the core things too, is that we want engineers to think about the physics side with the security, so that even if an attacker got in through all your controls, the physics won't allow something to happen. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 168 of 316 |  |
|  | | | | | | |
|  |  | P5 |  | And and you can and and you're you're basically doing it by through questions to be answered rather than through any list of things that must do, which was a problem with the earlier correction. | | |
|  |  | P5 |  | So yes, so you so you can you can actually attach a financial value to doing cyber, yes in that it it becomes a it does lead to tick box security but it it's better than no security. Yeah. | | |
|  |  | P5 |  | So there are two benefits, presumably of this one is you can write it into a contract.  You can say you know, in doing this you will please look at these questions and we would like some good answers to them. | | |
|  |  | P5 |  | These questions are more partially the answer to your original question.  I said I couldn't tell you how to do it, but that's part of the process that you're gonna go to come up with those solutions.  Again, we're not telling you the solution to use.  We're just saying, hey, you know, make sure that you can answer that.  You know your security controls that you put in place will protect the function, say, or whatever | | |
|  |  |
|  |  | P6 |  | I | | |
|  |  | P6 |  | Yes. Yeah, yeah. So Cyber aware engineering. Yes, yes, indeed. | | |
|  |  | P6 |  | The the the sign process the the the at the very beginning already should take into account the potential threats and risk and then you're building the start of building the system according to it. You know just implementing it and then let's see and somebody else will sort it out and allow the IT organisation which doesn't have the knowledge to know how the people, the money and the tools should then protect the system. It doesn't work. | | |
|  |  | P6 |  | So that's so you're saying it's an engineering. The solution comes in engineering in more up front.  Risk based analysis of problems, identification of problems and yes and. | | |
|  |  | P7 |  | Not. Not yet anyway, but I think this should be part of part of the mission. I think this should be part of the mission in digital systems. We haven't done this, you know.  You you probably you know, if you were putting bridges together, you you wouldn't be able to to get away with the equivalent of lousy software that a lot of us get get get away or many companies get away with producing these days, right? | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 169 of 316 |  |
|  | | | | | | |
|  |  | P7 |  | So it's interesting. Yeah, it's. So it's interesting that you say this because in other disciplines, resilience engineering is a thing.  So, so, so. So when I interviewed for for this Royal Academy Fellowship.  I can't remember exactly the the panel the the background of the people, but obviously you know the Royal Academy so covers all engineering right? And and when I talked about resilience engineering as a keyword, one of the panel said but you know in in other disciplines this is this is the thing already. And I said yes I do. I do know that and I wish it was a thing in in computer networks, but unfortunately it isn't. | | |
|  |  |
|  |  | P7 |  | So we're talking about.  Software resilience, engineering and a sort of new science on what what makes software, what makes systems more resilient, how you build that in automatically. | | |
|  |  | P7 |  | Resilience mentality. If you like that we need to protect, we need to have mechanisms in hardware and software in place that protect the operation of our systems and we need to accept that some of the resources and some of the of the electricity and some you know will go towards this. It's not, it's not going to be you know.  We we cannot, we cannot live without it. | | |
|  |  | P7 |  | But but but I think beyond the hardware beyond the these kinds of developments, we really need a, a, a sort of. | | |
|  |  | P8 |  | OK, so I now if I start answered I have to go back to the background of the even five days. Say human factors is pretty much is a profession like in itself. So to be able to do this job and other people are focusing on UX but essentially looking into the task of the user that you need to understand how to the whole task analysis for example you need to understand to look into like an environment you need to look into the humans, the skills and capability which is part of psychology and cognitive psychology. You need to look into Physiology. You need to look at all the other things. So yes. But what I'm trying to say that if I understood the right I mean.  It's around, but it's more sounds like for example, I'm asking you, can you trade me on cybersecurity? You could be, but then you have to understand the whole.  Topic behind so that's why I guess what I wanted to say was that more like cooperation between him, in fact with professionals for the psychologists and the cybersecurity engine, if I understood that if we just train, you will be seeing one part of it. So if we can tell you, look, make this system more simple. However, this context dependent again, you may be able to consider in one context if you train you for it, but if you don't understand the wider.  Fundamentals philosophy behind it, you may not be able to understand it. For example, in a nuclear reactor because you will not be looking for the things that we are looking for. Does it make sense? | | |
|  |  |
|  |  |
|  |  | P8 |  | Yeah, I'm really worried to say this because I know this will end up in a persona and then they will put a nice cute face that they are like young, female up at 2:00 AM. It was one of 600. That's not what I meant anyway. But yeah, it's just, yeah. Anyway, another thing is if you start understanding humans more and more, you know, like we didn't talk about of this, like, an autistic people or we didn't talk about, they say the dementia. So they all become more and more issue later on because humans are evolving. We are changing, we are changing. Look, we are getting older.  And this body it will. We have noticed when we did the cooking first, I don't completely too much but we are getting older. We are getting bigger. These are all scientific. I'm not making it up. Yeah, I'm getting heavier. This impacted for example having designed the stations. So the witches used to be small. Now we need bigger spaces to turn it on because the sign says we are changing physically. We're changing physically. We're changing cognitively. We are changing. We are changing a lot.  Genophysiologically. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 170 of 316 |  |
|  | | | | | | |
|  |  | P8 |  | I I would say so. I mean the reason why I say this is because they say this in a lot of user interface experts. They say that UX and so on. So they have the fundamentals of the design but they apply the same sort of principles for almost every context because maybe they don't look for different pith matching ages.  Different personalities or different context. Even the Physiology of humans. Do you know, like the hormonal levels change? They may be focusing on one thing.  But human factors is is taken into account, so I think they say we study Physiology, we study psychology, we study.  Environmental science. We work with the pretty much of like an architects, so we are looking into how this light may be affecting you, not only the system. So anyway, I don't want to get too much deep into it, but it's a profession. It's a all the degree because it's located on. My fear is, if I will tell you that you can get trained, it will end up to something like some kind of fear. | | |
|  |  |
|  |  | P8 |  | Games that the HCI, the, the psychology, the and some knowledge and an knowledge to be able to talk to the people who are also doing the cyber and the people who are doing the, the, the system's creation or or set up or management even. Yes. | | |
|  |  | P8 |  | OK, so so we're not looking for that sort of training. We're not particularly looking for people to come out of university knowing how to do your job. What we're looking for is cross discipline teams. | | |
|  |  | P8 |  | Yes, management. I mean I would say yes to cross functional teams. If you are looking at riders, I would get yes. So that's my view, yeah. | | |
|  |  | P8 |  | If you ask me, I say well, it keeps you up at night. I'm like, I'm seeing all these things. Either people don't see it or they see it, but they don't care, even though they care. They don't want us in the same field exam because we are very different people as I than they are. But we need to talk. I think lack of cooperation have I feel right. I know. I see so many things because I wasn't really prepared, but lack of cooperation between human factors, people, psychologists and the behaviour scientists and cybersecurity engineers and managers, really. Who is looking into all the CEOs of the C OS or whatever.  This is keeping my fit now, lack of talking if you ask me. Thank you. | | |
|  |  |
|  |  | P8 |  | So I mentioned the usability I mentioned like in other things, but these are all pretty much of like an underlying of try to understand the root cause. So to understand the root cause of either human error in a science that why the humans are falling for social engineering.  Is coming under. Why the human error have been stored? So what is the reason? I think all the efforts should be at this stage, at the very least.  To start, it should go there. Why human error is happening and underneath This is why are we falling for social engineering is due to our personality. Is it usability? Is it because the other guy is too sophisticated? There could be million reasons, but the question of why is that?  And really, pretty much when you try to like and understand the why, I would say.  Different discipline like the cross disciplines should really come together and pretty much.  So I can understand why this is happening, because you might be dead questions. A lot of mitigating strategies are being developed without really understanding why things are happening. So if you ask me where should we put our effort, I would say not. The question hasn't really answered yet. Everybody's finding a solution. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 171 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Need for Cross Discipline Communication** |  | | | | | |
|
|  |  | P22 |  | the role of it guys is changing.  In terms of what they need to be aware of and what their certainties and uncertainties are, and it puts a lot of emphasis on it, guys for being able to communicate those uncertainties to the budget holders and this is a big disconnect, it's a real problem. | | |
|  |  | P8 |  | I see so many things because I wasn't really prepared, but lack of cooperation between human factors, people, psychologists and the behaviour scientists and cybersecurity engineers and managers, really. Who is looking into all the CEOs of the C OS or whatever.  This is keeping my fit now, lack of talking if you ask me. | | |
|  | | | | | | |
| **Neural Computing** |  | | | | | |
|
|  |  | P9 |  | We might see our first our first adopters within 15 years. I | | |
|  |  | P9 |  | the I think I think AR and VR are a are a cul-de-sac. I think they're going to be a dead end.  That that you'll never be able to Add all of the elements of experience to a human being together externally. So I want to give you sight to taste sound I want to give you proprioception. I want to give you balance. I want to give you all of that. And I want to do that through external stimulation.  What's the point? I can go straight into your brain and make you think you just felt it. So inducing a qualia is going to be the way that we're experiencing a metaverse. Our dream world will be inducing a quality directly inside someone's head. It won't come through a set of arvr goggles.  That we've we've kind of done that and we've got as far as we're going to. And while we're living half in and half out of the metaverse, that could be quite a useful gateway drug. But if you're going to be fully immersive, it's going straight into your head. | | |
|  |  |
|  |  | P9 |  | ultrasound is already point directed. Ultrasound is already being used to stimulate parts of the brain. You can do it electronically. You could put implants in neural link and so on are playing that game. I mean, they're sort of quite late to it, I gather. But really, what's what's cracked it is the ability to encode information in a way that it hasn't effect. And if you try and do that in a structured way, by understanding the brain, you're going to hide into nothing because it's too complicated. But we pass that now with the way the transformer models are working, we're extracting the entropy from a massive data set.  Experiencing it in a contextualised form, skipping the bit of structuring it in between. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 172 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **New CNI and Changes to CNI** |  | | | | | |
|
|  |  | P11 |  | Well, you and you mentioned cloud. I think the only one that I think has really joined the.  Electricity, water and and and arguably gas is is now the Internet and I can remember.  About 2008, there was a discussion in in policy circles in the in in London where I worked at the time about whether the access to the Internet would become a human right.  Touch, but I suspect he probably has or it should be by now. | | |
|  |  |
|  |  | P12 |  | , I think that people underestimate how chaotic that would actually be. I mean, yeah, again, you know, you try to swipe your thing at square terminals and point of sale systems and they, you know, they don't work. So I worry a lot about that because I think that they're a great target. I think that it's within the capacity for, you know, AP TS to do.  And I think that it is perceived as not something that's going to provoke a kinetic response. I'm not sure that that's true, but I think it's perceived that way and that really keeps me up at night.  Because that's a world where suddenly I think everyday Americans would be under the impression we're under attack.  And again, this is the US context. I don't know about the UK as much. | | |
|  |  |
|  |  | P12 |  | whereas something like a content distribution network, you know, a lot of stuff is going to go down. People's credit cards aren't going to work. And, you know, apparently. | | |
|  |  | P12 |  | so Cdn's becoming critical infrastructure definitely is the biggest thing on my mind lately. Payment processors. So things like like the squares of the world becoming critical infrastructure. | | |
|  |  | P12 |  | It's not a bank failure. It's the opposite. It's you can't. If you can't get at it. | | |
|  |  | P12 |  | the major incident that always keeps me awake is really sophisticated state backed attack on a content distribution network like Cloudflare optimise | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 173 of 316 |  |
|  | | | | | | |
|  |  | P12 |  | And again, this isn't like a war thing, but say you're like an Indonesian short sell.  And you have an idea that you know you're not going to get caught on, all you need to do.  Is like get into Cloudflare or pay a cloud flare turn and say hey, can you change this BGP route for like 30 minutes and you you know do something where a big Indonesian financial firm is inaccessible for 30 minutes, make a lot of money on your short position exit your short position and then the issues are stored Potter says oh we're investigating but it just seemed to be a misconfiguration and you've made millions of dollars potentially.  Would you actually get caught? Like I really don't think so.  So yeah, I I do think that that I think that that's actually very possible. | | |
|  |  |
|  |  | P12 |  | So what I'm trying to illustrate here is like, although all we've all we've seen are \*\*\*\* \*\*\*.  That were like, just basically misconfigurations, if you know how the network fixed together and you're able to engineer a \*\*\*\* \*\*, you know, like an apt, it can be pretty hard to recover from actually, because if you're saying there's an accidental BGP misconfiguration can make all metapods offer a day, you know, again like a A team of Chinese spies. It was like, has nothing better to do but to figure out how to turn off metapods. You better believe that meta, like all meta products, are going to be offer a while.  You know, like you can really do a lot within the sabotage becomes intentional. And yeah, just these systems are more fragile than we expect. So what would that look like with Cdns with, you know, square? Whatever. Yeah. I mean, these systems could be down for days or weeks even, you know, if they're really, you know, putting intention behind this. | | |
|  |  |
|  |  |
|  |  | P12 |  | Anything that has has to do with CDN failure can mess things up, so you have misconfigurations. I mean this happens. This happens not infrequently, but like Acdn, will this configure something and like all of their customers go down? Of course the problem is even people who are not directly their customers may be rely on a font or a JavaScript library that is hosted by one of their customers. And then that thing goes down and causes this cascading failure. So yeah, misconfiguration of Cdns I mean.  Obviously, an apartment attack on Acdn and also you know, I I don't haven't specifically thought about this and because in part just I don't have sources inside this particular well actually I do have a source, maybe I should look more into this but company like square they manage these point of sale systems you know for all sorts of people and there are even point of sale systems out there that appear not to be square point of sale systems but actually rely on square because they they just use square APIs for everything and like you just wouldn't actually be that hard to get inside square and turn it off. You know I can't imagine that they're.  Ready for, you know, a Chinese apartment. It just. And again, maybe they are. OK, maybe they are. You know, maybe maybe cease is in there. Maybe they have former NSA people. But it seems very unlikely to me that that's the case. So yeah, you know, turning these kinds of of payment service providers off like.  I really it seems so easy to do that it seems unlikely that someone at some point won't try it in the next 5 to 10 years. Just be like haha look American capitalism doesn't really work. | | |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 174 of 316 |  |
|  | | | | | | |
|  |  | P12 |  | I don't think tech companies really are or if they are, then it's really, you know, secret even from media people in Cloudflare research don't know about it. If that if they are table topping those things, maybe they just don't know about it, but.  You know, financial institutions really are ready for the Internet to go down and also, you know, look, these financial institutions existed before the Internet.  They know about, they know about not having the Internet and still being able to do financial stuff. The problem that I see with money is that the way that we interact with money has this tack layer, this fintech layer in between. And it appears that we're just doing transactions, but we're actually dealing with Block, Inc or we're dealing with whatever the \*\*\*\*, you know, that that that is interposing themselves between the financial institutions and us and to some extent, the financial institutions have sort of encouraged this because they have this, like, white label system where you can kind of get their white label fight this again, us. OK. I don't know about the UK.  The US these big, you know, settlement banks have these like white label services that they all can compile. You know these APIs or whatever super convenient in the US you can log into any financial institution from any other with Plaid. But what this really means is that there are these like small startups interposing most people's transactions against these financial institutions, which is fine for the financial institutions. When the Internet goes down, their money's all safe and they can be. Don't worry, your money's safe saying this. But from the perspective of someone buying gas at the gas pump.  My money doesn't work. I don't have access to my money. I can't spend any money that causes a freak out. I think so. That. That's. Yeah. And of course, all of those things are now relying on Cloudflare, Akamai. | | |
|  |  |
|  |  |
|  |  |
|  |  | P13 |  | And if you think about how, for example, medication is supplied and distributed, that's critical part of infrastructure. Same with things that are like PPE, for example, when you saw that through COVID. So I think I think that the whole supply chain.  Across the NHS that keeps it functioning is probably, yes, critical. | | |
|  |  | P14 |  | public spaces and critical public spaces and sports arenas, concert halls and the like. Those areas in rather generic terms seem to be being swept up into the under the umbrella of critical national infrastructure to a degree.  I don't know if that's formally the case, but you've I've sensed that happening.  And so things like the what used to be the centre of the production of national infrastructure certainly started getting involved, as I recall, in worrying about arenas. Partly, I think because of the threat being seen back to our very beginning of our conversation, because it was judged that certain iconic buildings.  Carry a critical a national significance.  They then become woven into the idea of being part of the critical national infrastructure.  Muddle thinking, you might argue, but nevertheless it could be that hitting.  Wembley on the day of the FA Cup final would be far more significant, at least in political terms and in terms of the impact and keeping people awake at night than hitting a major power generator, which is part of the infrastructure. | | |
|  |  |
|  |  |
|  |  | P14 |  | But it does change.  The map of what is critical in a sense right the the map of who is delivering critical services or is it? Is it actually? Because if, if, if everybody was delivering those critical services, perhaps they don't become critical anymore or something new becomes more critical. I don't know the way that the network delivers that stuff around. | | |
|  |  | P15 |  | so we need to think about that differently to actually everybody gets their electricity off a grid which runs off a power station and all of the power stations have gone down and we're going to be in on an operation Black Star and it's going to take us three weeks to get all of them back up and running again. And it's like systems for turning one and getting one started. And that empowers the other fight, like the other five in that empowers and all of those things. So, like, the way that they're all set up and the way that those.  Critical services.  Are delivered impacts.  Exactly what it is that what it means to be critical. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 175 of 316 |  |
|  | | | | | | |
|  |  | P15 |  | that comes down to your definition of.  Of what it is that you're trying to achieve, and therefore if you like the things that we're trying to achieve haven't changed, I don't think we're just going about doing them in a different way than we might have done.  Before in terms of effectively like shopping.  A A physical shop on it. Opening its doors is important if that is how we do shopping.  Hmm, drivers and lorries and deliveries are important if that is how we do shopping and we don't go anywhere. So, so that the wanting to like the need for.  Like essential provisions hasn't changed. It's just we have changed how we do it and therefore.  The the things that become critical, they become critical because they're delivering a service. | | |
|  |  |
|  |  | P16 |  | Computing systems directly anymore, but they rely on 3rd party providers.  Of which they know very little about, so it's easy for a bank to ask to see what's happening in the systems of their partner financial traders, because everyone has to abide by the same type of regulation, and so they trust each other. They know they have to operate, but then it's impossible to ask a financial partner institution to have access to their Microsoft.  Or IBM or Amazon cloud.  Services because those companies are much bigger and they say no, no, no, we just provide a service to you. Trust us. You know, we have thousands of engineers, so it's creating.  Lack of understanding of the the reliability and so the cloud computing. And now I think in the I think in the in the US the the the financial sector regulators are now asking submitting the cloud computing companies that service the financial sector.  To some high levels of oversight as well.  Saying that, if you want to enter this business with a financial.  Institutions, you're going to be part of the packet you're becoming part of the package now, so we're going to have to ensure that you deliver certain levels of services according to certain requirements. I think that the cloud computing, because it's introducing another layer of. | | |
|  |  |
|  |  |
|  |  | P16 |  | Complexity.  And very often by companies that come from very different sectors, from very different understanding of what security is about. And it's very.  Very sophisticated companies because of the levels of investment required and they're very hard for the customers to really know what's happening in those data centres and to really have a guarantee of their so. So I think really cloud computing would would be.  For me, the the really critical.  Component of of of those? Yeah, as a trend, it's something that it is really super important. | | |
|  |  |
|  |  | P16 |  | Yes. And I would, I would say more the cloud computing than the than any other sector, it's it's something I've actually.  Tackled in my work on cyber resilience with the banks because the so now for.  Economic reasons and cost efficiency reasons.  All organisations are using heavily, depending dependent on on cloud computing solutions. The problem is that when you have a financial so when you have a critical infrastructures are usually very heavily regulated.  And for a good reason, so that the regulators and the state ultimately want to ensure that they put in place systems to maintain high levels of reliability and we can have confidence in their ability to deliver critical services to to the population, what is not so heavily or so.  Meticulously regulated are those.  Cloud computing technologies, upon which those critical infrastructures more tend to rely more and more. So what we found is that the banks are very worried, for example about their.  Ability to guarantee that they will keep on being able to trade even during a crisis, because now they don't control. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 176 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | More forms of infrastructure becoming critical.  Such as E retail perhaps, and COVID we found or cloud computing services.  Is that is that a trend you see being important here? | | |
|  |  | P20 |  | And the way I think about it is what is critical to the effective and safe functioning of society. If you turn something off, what what is going to lead to a societal failure or or loss of life to a significant degree. So it's the things that are critical to keep operating, to enable society to function. I guess that's the way I'd think about it.  I noticed the NCSC have their own kind of web page on C and I and how they think about it and defining it. I imagine it's not dissimilar to to the way the US defining it, and indeed they they cite Jenny Lee, who's director of CISA, in that Web page. | | |
|  |  |
|  |  | P20 |  | the American Government understand it is they take a sexual approach to what is critical in that national infrastructure. I don't know whether they have a specific definition of of the term critical infrastructure or critical national infrastructure, but it's my understanding that they look at it in sort of a sectoral way and look to define which sectors constitute critical nap national infrastructure because of course then Department for Homeland Security, for example, then has a mandate to protect | | |
|  |  | P20 |  | The things I'm probably most concerned about at the moment is election security and and the security of democracy. | | |
|  |  | P20 |  | You know election systems now I believe are listed as critical national infrastructure in the United States.  Do you know how I've inter Internet service providers themselves? | | |
|  |  | P20 |  | So if you look at critical infrastructure on the Homeland Security website, they talk about networks of highways, bridges and tunnels, railways, utilities, buildings.  Transportation, commerce, clean water, electricity, et cetera, et cetera. But I think actually their definition has widened to include things like again Internet services.  Election systems and a governance infrastructure around elections and various other things. So I generally tend to look at the CISA definitions, or reference to CISA definitions, or the Department for Homeland Security ones. I may be a bit US centric in that regard, | | |
|  |  |
|  |  | P20 |  | I mentioned before, as a broadening trend, there are increasingly increasingly things that are categorised as critical national infrastructure when they haven't been before. You know, I'd probably put cloud computing in the in the Internet service provision bucket as you were. Obviously it's part of integral part of what's offered by Internet service providers now and.  And I guess for a long time, the cloud security thing has been quite quite prominent. If we shift all our data to the cloud, does that make it safe or not? I've never been entirely convinced it does.  So yeah, look, I I think that that's.  You know that's a worrying trend and you know, not least because the amount of data that's now stored in the cloud provides these vast repositories, which can be exploited for, for AI and used to to teach AI. So we've got a sort of a conflict emerging about access to data.  And how data is managed, particularly the data that's stored in in the cloud, as it were, which again, most people seem to say whenever these conversations happen.  Obviously it's not a cloud, it's a. It's a big room with a load of servers in it. In the United States predominantly.  I worry about European dependency, particularly on American cloud service provision. This is a problem. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 177 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | both during COVID, but then also in our ransomware incidents, we've seen that education and also particularly schools as also a measure of daycare like it's not just not just the teaching bed, but also the daycare, the family structures, the way society functions on a day-to-day basis.  That they are sort of critical.  Central to yeah to our societal structures | | |
|  |  | P23 |  | US makes a critical distinction between events which happen all the time, right?  Like and what is typically referred to as a material breach.  And so I think that the beginning is gonna be to start reporting.  Material breaches.  And you know, to kind of switch to the technology side, the.  Umm, the challenges run so deep because.  I'm a lot of different systems in the US are provided regionally or even on a state level.  Umm, so we have a multiple electrical grids and infrastructures and water and so on. | | |
|  |  |
|  |  | P23 |  | from a US perspective, we have a lot of critical infrastructures.  I believe there are 16 different categories of critical infrastructures.  Well, there's a catch.  All government critical infrastructure that includes justice systems, voting umm, the military and so on.  But then there are all these other a verticals.  That include everything from what you need to live like energy and water, two things like umm, large commercial establishments.  So in the US, if you run a shopping mall, you can.  Ask for critical infrastructure protection. | | |
|  |  |
|  |  | P3 |  | So that that sort of notion of what is a critical infrastructure or you know critical service provider, you know it sort of shifts a little bit.  If you start thinking about it in those terms, you sort of need to widen the net a little. | | |
|  |  | P3 |  | if if you target a kind of, you know, I don't know distribution system operator directly or or a nuclear facility directly.  That's really hard, but if you tag in one of those suppliers, it's maybe a little bit easier and he gets you away in right? | | |
|  |  | P6 |  | But that we have five global actors, which is a monopole at the end. | | |
|  |  | P6 |  | And everybody from private to industry, even to public, is using these cloud infrastructures.  And losing the whole serenity completely, that kid could not be the future. We are there at the moment. I don't believe that this will work from the business models will not work, but also from principle call IT security point of view. So the so the the, the the data's around The Who who owns the data who controls the data to build business on it but also to use it in our call it democratic systems it will not work if we completely give up.  The way how we control the data, that's the biggest challenge now how to deal with it. | | |
|  |  |
|  |  | P6 |  | Classically, in broad terms, we are not part of it, but at the same time, we use the big cloud providers and we give out our and when we lose our data sovereignty, that's unbelievable. So that's a completely mess of understanding, I would say. So especially because we have all these privacy concerns in our systems, we have to find new means. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 178 of 316 |  |
|  | | | | | | |
|  |  | P7 |  | you know the Internet and and telecoms and networks.  Are not a playground anymore. They were a playground for years for researchers like us and for for people that you know, they were using it as a sort of global entertainment system.  But now you know this system is is the backbone that you know, lots of businesses make money from, you know, big tech.  You know my.  My house sitting is is controlled through that. | | |
|  |  |
|  |  | P7 |  | I'm afraid that it will take failures and attacks and disasters.  To to to convince the global, the global public that that this is the case, or the policymakers for that for that matter. | | |
|  |  | P9 |  | Metaverse and the spatial Internet, where a digital twin of everyone and everything, bits move, atoms move with the speed of bits. And we're basically living in this mixed corporeal and digital world. That means that our society has a digital representation and a model.  Information model the taxonomy and ontology a set of standards. That is a piece of critical national infrastructure which needs to be protected because of that information model fails. It'll have. It'll have real world consequences.  Again, it's it's somewhat less tangible than saying do you mean like the banking Ledger in the Bank of England? OK. Yeah, yeah, that too. But really, it's all of those sorts of things. So yeah, I'll put those two. I'll put. I'll put that that down as a marker and say for those two reasons, the information model of the country itself is a piece of national infrastructure. Also say then thinking about.  The economy and finance, so many of the services and systems and economic mechanisms that we use today are now running on a data infrastructure that could fail every. So the network and everything else, their information model matters. | | |
|  |  |
|  |  |
|  | | | | | | |
| **New Nuclear** |  | | | | | |
|
|  |  | P11 |  | Environments like Smrs will only be economically viable if they use technology that isn't currently regarded as being appropriate to those kinds of.  Safety critical environments, so you can't always get the sensors you want and the places you want. You can't always have individual wires going to every last sensor because there isn't the space and they're sealed for life.  So you end up having to do in make inferences to parameters rather than.  Bring them directly. May not be able to measure a particular pressure in a particular place. You may have to make some form of inference.  Using and here it comes using a digital twin.  And and so I see quite a lot now that's that's a sort of development beyond what I referred to earlier, which is that prognostication prognostics and diagnostics there we are.  The prognostics and diagnostics are effectively done, even if they may not be advertised as such against a digital twin.  And I think the question is. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 179 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | Yes, yes, course so. So it's all of that kind of. Oh, but it's an improvement. Well, not to me it isn't that kind of problem.  So let's see. We've talked about that. We've talked about the cloud stuff.  There's another area I want to go into, which is.  Let's let's extend the machine learning area. So one of the areas that I'm I wrote, I wrote something about late last year was.  How computer security will need to step up for a small modular reactors for Smrs and?  I I didn't just sit at home and dream this all up. I I actually helped run a meeting in. Well, actually at EDF in France, which had lots of international people come and talk.  So I gleaned a lot from then and.  The there are there are many areas I think of concern, but specifically to your .1 of the areas that will need to concern us is that. | | |
|  |  |
|  |  | P14 |  | For | | |
|  |  | P14 |  | so we we have our CNI right now.  I don't have much.  To contribute here, other than to ask the question, this might be good rather than a bad thing. Are we going to be seeing a?  Decentralisation of the delivery of.  And the operation of some CNI services.  The first thought I had was around.  Electricity. So I think we're going to be seeing. I hope we're going to be seeing the proliferation of micro nuclear generators.  An even more micro level. | | |
|  |  |
|  |  | P3 |  | Something with a larger footprint, but for example microreactors the the kind of idea is that they might set on the back of a truck.  So these things could be mobile, yeah. | | |
|  |  | P3 |  | generally speaking, so the idea is it's, it's the kind of one of the sort of core concepts is that the the, the SMR is sort of prefabricated if you like off site by a manufacturer, let's say General Electric or Rolls Royce or whoever it is. | | |
|  |  | P3 |  | And then it delivered to site and then put together constructed so that that kind of IKEA flat pack type. | | |
|  |  | P3 |  | The other thing that they're trying to do with these things is that the sort of in order to make them a little bit more cost efficient and everything else.  And I think sort of enabled by this change in the safety kind of set up is allow them to be kind of remotely operated or have multiple modules upgraded perhaps by 1 control room. | | |
|  |  | P3 |  | So this kind of like changing the safety setup, changing the way that we want to operate these nuclear facilities, some of the applications of them and stuff kind of allows or invites or requires us to start to use kind of new digital technologies and by and we're sort of at the stage where it feels to me like the sector is sort of.  I mean, yeah, sort of trying out ideas. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 180 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | But the kind of but the kind of the idea with these sort of SMR and these sorts of technologies is that they're supposed to be smaller footprint, easier to sort of get regulatory approval for and sort of and and therefore a little bit cheaper and easier to sort of deploy than sort of large traditional nuclear facilities. | | |
|  |  | P3 |  | Yeah, there's sort of, yeah, the, the kind of fundamental thing that I think is supposed to have changed.  And if you believe believe the types are to say is that the sort of safety equation with these things is sort of changed quite significantly in terms of the nuclear design in the sense that if it's not actively controlled, it's sort of self cools, right? | | |
|  |  | P3 |  | so the so the so the so the things that they're talking about, some of the things that you know I'm sure you've heard before you know, so the application of machine learning for this space autonomous operations sort of implies artificial intelligence or some form of autonomy. | | |
|  |  | P3 |  | So I mean, yeah, I OK my, my my opinion is it was sort of rather not very complicated but but basically there was a suggestion that foreign nations had to sleep a malware what they were calling sleeper malware sort of starting systems at Southfield.  Well, that's not good. | | |
|  |  | P3 |  | You know the use of cloud potentially kind of associate that also with you know the use of digital twins, which is a sort of a kind of a hot topic if you're in that operational technology space.  Sort of telecommunications, right?  Which is sort of not really a thing that people.  I've I've sort of thought about too much in kind of nuclear before, and then things like uh, you know, sensor networks and in particular kind of wireless sensor networks or wireless instrumentation and control. | | |
|  |  |
|  |  | P3 |  | And and it's sort of nature of the threat that sort of kind of while you know there's there are additional kind of risks that from cyber point of view that wireless introduces that.  But there's this sort of kind of space.  So one of the sort of issues with this smars and microreactors in particular is that you don't have an awful lot of space for for equipment.  So that sort of pushes sort of people to think about kind of wireless sensor networks and stuff like that because you don't have kind of maybe as a support, I mean again, so this is all ideas that at some point need to hit regulatory reality. | | |
|  |  |
|  |  | P3 |  | I could, I think if you know outside of just doing the, you know doing the the the trip or whatever it is that just to disconnect to contain the issue.  We sort of really need to understand what's happened really quickly. | | |
|  |  | P3 |  | Most of the scenarios that I've kind of thought of that we thought about in the nuclear space, the kind of, yeah, it's some controlled or uncontrolled trip over the reactor, right? | | |
|  |  | P3 |  | You know, how do you go about determining that you have sort of trustworthy systems after after the fact.  It's a kind of a major, major issue.  Like, have you really found all the compromise systems?  Do they still have some latent capability?  You know what I mean?  And and kind of those sorts of things that are more about sort of response and resilience in a sense, yeah. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 181 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | So you know those sorts of things are slightly worrying, right?  And and it extremely difficult to detect, right.  And so yeah, those those are the kind of nightmare scenarios, I suppose that were that we would be worried about, I suppose, yeah. | | |
|  |  | P3 |  | And you know, it's blackouts or or or that sort of thing. | | |
|  |  | P3 |  | And if you have the likes of SMR, which would so so the kind of general conversation with SRS is, that's possible.  Remote small nuclear safety.  Sort of sort of.  Equation has changed.  Then there's sort of risk shifts little bit to be more about nuclear safety like you have this thing in the middle of nowhere with not many staff an increase risk of somebody sort of stealing material. | | |
|  |  |
|  |  | P3 |  | Denial of service. | | |
|  |  | P3 |  | And if you're using digital systems to support remote surveillance, physical protection systems, or this kind of stuff as part of a blended attack, then theft of material is becomes a bit of an issue.  And then the other kind of sort of potential shift in and kind of concern is around availability, right, energy security, right?  So if we if we, if we don't, if we can't necessarily, you know maybe we don't.  Our attacks don't result in, you know, release of material or anything, but we could put the thing off off grid, right offline. | | |
|  |  |
|  |  | P3 |  | And and if it's, you know the the sort of issue with with, if it's a cyber, if it's a cyber problem, you know the major question is to what extent is the system trustable thereafter, right?  Can we just simply switch it back on again?  Probably not, right? | | |
|  |  | P5 |  | And that opens up to, you know, outsiders in between the reactor and the control room, which may be Colomiers away, you know, anybody can now the physical protection is very different than posting guards or whatever at a facility.  So I think that's where my #1 push would be.  Is that remote communications? | | |
|  |  | P5 |  | I hope it's not controlling the reactors, but I hope it's only informing them and there's conversations about that. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 182 of 316 |  |
|  | | | | | | |
|  |  | P5 |  | Umm, but for me the biggest one that's more immediate is the remote communications because when you have multiple SMR's in a geographic area, they're talking about having maybe one control room that feeds to all of these reactors.  And so how do we secure those communication lines?  You know whether it's hardwired or wireless or whatever it might be.  And you know, it's not just monitoring, but they're looking at control through these remote communications.  And so that's gonna be a really big deal to verify that we can convince people that we have a cyber secure communications network there.  And then the last one is just really quick before I get it in before I lose it is autonomous operation and that's where maybe the AIML type technologies will come into inform the operator. | | |
|  |  |
|  |  | P5 |  | Umm, they're talking about, of course, the use potentially of AI, machine learning, digital twins. | | |
|  |  | P5 |  | So in nuclear, I'm involved in a lot of advanced reactor research with small module reactors, microreactors, things like that.  And having been a part of those workshops and conversations, they are talking a lot about wireless technologies.  They're talking about using 5G dedicated 5G networks. | | |
|  |  | P5 |  | And | | |
|  |  | P5 |  | So let let's just take AI or digital twins right now if if people wanna use that technology to help the advanced reactor world for good purposes, great.  But from a security perspective, how do you trust back to the trust?  How do you trust that that digital twin hasn't been manipulated by a cyber adversary to give you the wrong results?  How do you not know that if you're using AI to make decisions to run a reactor that it's not, it didn't make some weird?  Connotations on something and says, hey, today I'm going to operate totally differently. | | |
|  |  |
|  |  | P5 |  | So I would say my first immediate one to research would be that remote communication link to make sure that's that's as secure as possible.  And I say that because we're kind of going through a nuclear renaissance right now with the old big reactors to the smaller reactors.  It's all new type of design.  They talk about the passively safe properties of these, where there's no matter what, it's not gonna go and melt fuel or anything. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 183 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **No Understanding of Analogue Engineering** |  | | | | | |
|
|  |  | P18 |  | one of the consequences of the shift towards digital.  Is that a lack of competency?  A lack of competency around analogue systems, so we no longer or we got a very much reduced capability in the UK for analogue electronics.  Because lots of training and stuff goes towards.  Digital. Yeah. Yeah, people coming out of degrees don't necessarily understand analogue electronics. They're mostly dealing with digital things. | | |
|  |  |
|  | | | | | | |
| **No Understanding of Cyber Risk** |  | | | | | |
|
|  |  | P17 |  | cyber risks is a bigger problem now than it is yesterday and will be tomorrow.  And I think people are sort of aware of it, but I think the problem is is not necessarily, I think if people hear it too much, the the kind of actual need for it doesn't necessary sink in too much as well as the well as the understanding. | | |
|  |  | P20 |  | In terms of.  Software development for critical infrastructure. I don't know a huge amount about it, but historically it appears to be riddled with vulnerabilities and weaknesses in terms of if you look at the state of secure software in those sectors.  Not a lot of protection around lots of industrial control systems. Wanna cry virus spreading globally affecting the NHS, systems that are still running Windows XP.  Legacy software not being able to update it being used globally, which of course creates a whole new, you know, levels of vulnerability.  Yeah, I mean, I I just think it's a, it's a market which.  Is pretty pretty weak still in terms of security | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 184 of 316 |  |
|  | | | | | | |
|  |  | P22 |  | You're familiar with it and understand the problems and people who are not familiar with it and don't have the vocabulary to understand it. And it's probably a vocabulary around systems thinking rather than it specifically, but certainly.  If, well, again, I was saying that which spent several hours in discussion with policy advisers in gsit, and they were really nice guys. You know, one of them had an MA in measure Portuguese mediat, I think, and seamlessly gsit policy advisor on supply chain software supply chain. And actually she turned out to be quite bright because she came to a workshop and she had actually got it. But.  I shouldn't be having to be teaching people about.  You know the others are. None of them had any sort of STEM education, OK. And so systems thinking is a bit difficult if you don't have any of that. And so this was saying, well, she happened to be having a meeting of her research groups. And between them they listed like 130 people across the various government departments they work with. Now, remember, she is focused on infrastructure. So this was transport, this was.  Probably Ofcom. I don't know. So the 130 people and none of the people that they were in contact with had shown background.  Now this is quite frightening because I think it's quite a big change. I mean, certainly people I knew with science backgrounds went into the civil service.  Maybe they've all mustered out. I've been forced out because they didn't have the right rear path or whatever, but it's a big lack and you know, without that sort of thinking | | |
|  |  |
|  |  |
|  |  |
|  |  | P23 |  | So the needs of the different stakeholders differ a great deal.  There are more and less sophisticated stakeholders.  And I'm sorry that this runs a bit against your that the kind of motivation of your study, but these bodies don't need protection from quantum computers because they're not even ready for basic cyber security. | | |
|  |  | P23 |  | There's like there are very very basic things like her.  Have you can have you allowed your control infrastructure to be connected to an Internet?  Resource like the most basic A that are not fully ironed out and the attacks against these infrastructures tend to be really basic stuff, not quantum stuff.  I'm gonna find you on LinkedIn and I'm gonna send you an email and ask you to log into the control site or the other.  So it it we really are at at our infancy and and and one of the questions, one of the great questions out there is why why haven't we had a disaster?  Umm the and there is some speculation, you know, like why haven't we had a dam loose control and kill 1000 people and the there is speculation that in fact many of these institutions do not but the you know the larger ones have not connected their control to the Internet | | |
|  |  |
|  | | | | | | |
| **No Understanding of Software** |  | | | | | |
|
|  |  | P19 |  | they'll send it engineers out to prepare the field unit or whatever.  No, they they have the they have that kind of will handle but that that that is relatively easy compared to some of the these more complex systems which software systems which may be subjected to.  To tax of a different sort or yes, or accidents of a different sort.  And where, of course, the traditional industry experts are not trained to know about problems in software. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 185 of 316 |  |
|  | | | | | | |
|  |  | P22 |  | You're familiar with it and understand the problems and people who are not familiar with it and don't have the vocabulary to understand it. And it's probably a vocabulary around systems thinking rather than it specifically, but certainly.  If, well, again, I was saying that which spent several hours in discussion with policy advisers in gsit, and they were really nice guys. You know, one of them had an MA in measure Portuguese mediat, I think, and seamlessly gsit policy advisor on supply chain software supply chain. And actually she turned out to be quite bright because she came to a workshop and she had actually got it. But.  I shouldn't be having to be teaching people about.  You know the others are. None of them had any sort of STEM education, OK. And so systems thinking is a bit difficult if you don't have any of that. And so this was saying, well, she happened to be having a meeting of her research groups. And between them they listed like 130 people across the various government departments they work with. Now, remember, she is focused on infrastructure. So this was transport, this was.  Probably Ofcom. I don't know. So the 130 people and none of the people that they were in contact with had shown background.  Now this is quite frightening because I think it's quite a big change. I mean, certainly people I knew with science backgrounds went into the civil service.  Maybe they've all mustered out. I've been forced out because they didn't have the right rear path or whatever, but it's a big lack and you know, without that sort of thinking | | |
|  |  |
|  |  |
|  |  |
|  | | | | | | |
| **Only respond to regulation** |  | | | | | |
|
|  |  | P10R2 |  | People in in well, in, in the sectors that you know that that I intersect with. These are good people. They don't just wait to be regulated. You know they they that that that good humans the commercial sector waits to be regulated but these guys know what's at stake and and you know even absent you know regulations that they would do good you would want to do you know good things so that was my that was my disagreement that but probably somewhat I'm somewhere between strongly and somewhat I think as I say.  These almost self regulating I mean obviously we don't we we we wouldn't ever conceive of that model and then commercial interest would of course sweep in. But I I think this sector is is has integrity and it's not regulation that kind of keeps it keeps us, it keeps it on the on the on a good path. | | |
|  |  |
|  |  | P11R2 |  | That being, no other issues, yes. | | |
|  |  | P11R2 |  | Yeah, and and it was extremely difficult to to move this individual away. He'd been in the industry 40 years and he was a senior designer for a company anyway. We must move on. | | |
|  |  | P11R2 |  | Yeah, I was in. AI was doing an audit in the finance in a very big financial institution. And I asked the head of something or other what is top risk was and he said.  Fine risk of regulatory infraction. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 186 of 316 |  |
|  | | | | | | |
|  |  | P11R2 |  | Yeah, I work for a risk management software company at one point and it was. It was shortly after one of the big banks had gone down. And I said, what do they think of that? And and they said, yeah, well, they refused to go and buy our our system. So it wasn't surprising that they had no risk management, I think. Yeah. Yeah.  It is interesting. Yeah, that, that, that, that banks do do that. That's really that's really odd actually, yeah. | | |
|  |  | P11R2 |  | Well, I mean, it's not just them. If you look at the nuclear industry.  It's a separate anecdote.  Try and extract the anecdote from the complex background so it was essentially a discussion about best practise in information security in the nuclear sector and no, no that system sorry secured by design in the nuclear sector and the process diagram for the person who's leading the discussion started with asked the regulator what we have to do. | | |
|  |  |
|  |  | P11R2 |  | There have been nothing else. There is nothing else. There is no other starting point for the process of design. | | |
|  |  | P11R2 |  | I said, but what about what? What about, you know, going out of business for other reasons? It didn't occur to him. No, as far as he was concerned, risk management in his to his board was entirely about the regulator penalising them. | | |
|  |  | P12R2 |  | Organisations and highly regulated sectors tend not to be proactive but wait for regulation to find Earth. I have no opinion about that. I've never worked in a highly regulated sector. I've only ever worked in like the Internet, which is not completely unregulated, but not not nuclear, literally. | | |
|  |  | P16R2 |  | Yeah. Well, the regulation, it's it all depends on the quality of regulation. So they respond to regulation, but you can have a, a, a compliance only response which is a very. | | |
|  |  | P16R2 |  | Are really trying to implement the letter of the regulation, but also the spirit, to ensure that they are staying ahead. So yes, they respond to regulation, but probably needs to be impacted a bit more because responses to regulation can vary a lot and should be kind of there are very varieties of responses to regulation. So that's why I was like trying to introduce a bit of nuance in in my assessment of the statement. | | |
|  |  | P16R2 |  | Kind of formal response, but doesn't really do much to improve the resilience of the system. And then you can have a more of a outcome based response where people understand the spirit of the regulation. | | |
|  |  | P17R2 |  | They're very driven by compliance, so if compliance is written into law.  Or or. It's not necessarily written to law, but it's it's like this is what we're building a compliance framework against. They're more opposed to complying with that than looking at risk assessments or risk based approaches, whereas in the West. | | |
|  |  | P17R2 |  | Yeah, I see it more in. It's a really interesting prospect actually from the West to the east that we're doing a lot in the east at the moment is in Middle East and. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 187 of 316 |  |
|  | | | | | | |
|  |  | P17R2 |  | And you somewhat agree that they only respond to regulation. | | |
|  |  | P17R2 |  | You can have things written in law, but not everyone understands it and not necessarily everyone has to fulfil it. Sort of. It doesn't feel like there's a yeah. So it's it's a really weird one, but generally speaking, it tends to be not as proactive as we expect and it tends to sort of be led by a kind of compliance led direction. So yeah. | | |
|  |  | P18R2 |  | Organisations are re regulated, such as nuclear, yes.  Look at what? Yeah. So in ONRI was head of innovation. | | |
|  |  | P18R2 |  | OK, I see. But it's good to put some things that are provocative in. Yeah. So that's that's that's good. | | |
|  |  | P18R2 |  | There's us trying to get on the front foot to understanding where innovation might happen and what the regulator needs to do about it. So I I, yeah, I disagreed with that. | | |
|  |  | P20R2 |  | Yeah, I've put somewhat disagree. I mean, I guess I think that they they are proactive in those sectors, but it varies across the sectors. I think probably the nuclear folks are more proactive than the health folks.  So there's differentiation between the sectors mentioned. Again, this is anecdotal. I don't have statistical evidence to back this up. But yeah, I mean, I would say probably a few and the nuclear sector, you're pretty proactive about putting in place measures to protect your infrastructure.  Umm, probably energy too. But umm, I don't. I think the health has been somewhat negligent, so I'll put somewhat disagree.  And you do want would like me to elaborate on the answers. | | |
|  |  |
|  |  | P22R2 |  | And so, yes, you're right. So the the sort of the guiding thing about what's coming out of this work is it actually all depends on keeping the electricity going. | | |
|  |  | P22R2 |  | Well, electricity is it because all the electricity regulation has been about keeping consumer prices down and it's only recently that the regulator is starting to talk about net zero.  Emission and it will be really nice if at the same time there were reliability. | | |
|  |  | P22R2 |  | But telecoms isn't telecoms is not very regulated really in that way, so they might. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 188 of 316 |  |
|  | | | | | | |
|  |  | P22R2 |  | Exactly | | |
|  |  | P22R2 |  | Absolutely yes. But again, I mean, you know my scope is, is is CNI and is these these fairly regulated in things, yeah. | | |
|  |  | P23R2 |  | They gave example of of water.  Water provision in Florida, where there's apparently lots and lots and lots of private water providers. But most people like as a as a percentage of population are using the municipal water company. Even if there's 100 private competitors. So it it's a it's a study, it's it's not really a study. It's more like A blog post done by Rosensweig that. But it does have some.  It it does have some, a couple sensible anecdotes to draw upon that instead of counting CIS, maybe we should be paying attention to the most dominant CN is. | | |
|  |  |
|  |  | P23R2 |  | Interesting refinement there too, like.  Rosenswig wrote has this interesting report where he points out that.  You know, in the US, people say most.  Cni is in the private sector.  But that is subject to.  Massive footnotes, including the idea that most C and I might be in the private sector but the most used CNI might be in the public sector. See, it's a really interesting point. | | |
|  |  |
|  |  | P23R2 |  | Yeah. Alright. So it's more on the nature of the particular sorts of CNI and whether it's a monopoly or not, that's that's really going to be the the choose and not that it happens to be CNI. Yeah, OK, makes sense. | | |
|  |  | P23R2 |  | Yeah, it it's it's the qualifier on only I. I do think that you know, there's your traditional monopoly, but then the where you do have competition like you know one example in EU SS healthcare.  Another is telecommunications. I I think in telecommunications, I haven't seen it in healthcare, but there is security awareness and and and mitigations that are occurring in telecommunications that are significant.  But yeah, I think where you have a when you have a monopoly.  A highly regulated monopoly.  You're kind of stuck. | | |
|  |  |
|  |  | P3R2 |  | In in the in the main, it's probably true. I would say regulation definitely drives.  Is is the driver right and?  And I think possibly.  It's very sector specific.  Right. So if you look at health there for example, I would say that health is a sector is significantly more proactive than maybe some of the other. You know what I mean. | | |
|  |  | P3R2 |  | Thought. Yeah. Or are they proactive or just just sort of more?  What's the word I'm looking for?  Well, the proactive in in terms of sort of.  Say digital innovation or something along those lines, right?  Maybe then other sectors that are perhaps sort of embrace that because of regulatory needs or or whatever. But yeah, for the most part, I think you know these, these things tend to be kind of driven a little bit by by regulation for sure.  Or guided or steered by regulation anyway, that's yeah. | | |
|  |  |
|  |  | P3R2 |  | Yeah, yeah, yeah, exactly. Yeah. I mean, I, I guess, what, what, what you probably get is a conservatism in the sense that.  Probably some of these operators don't want to move until the regulation is clear. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 189 of 316 |  |
|  | | | | | | |
|  |  | P3R2 |  | You don't. You don't want to waste time and money on something, right? You know that that that might be a sort of a contributing factor to maybe to some to some sort of conservatism in terms of, you know, technologies or solutions. It's like, well, if if it's not going to help us from a regulatory point of view, why would we sort of? So they want clear signalling, I guess is the sort of.  The thing? Yeah anyway. | | |
|  |  | P4R2 |  | Because you can't trust industry on their own to to do stuff. Secondly, is people might try and game. | | |
|  |  | P4R2 |  | Things I mean and the Boeing 737 Max thing is an example of of of of where that might happen, yeah. | | |
|  |  | P4R2 |  | Well, it's not the regulator's job to tell people what to do. I mean, if you look at a worthiness, for example, I mean, if you want to, if you want to fly something within the infrastructure, you've gotta get it. You've gotta get your your platform or aircraft, whatever, signed off by the regulator. It's safe.  They're not going to tell you what you need to do or they'll tell you is if your thing is if they repeat to to actually sign off your case or not. | | |
|  |  | P4R2 |  | Yeah, I'm inclined to agree to that as well, because I mean, in theory in theory, we.  You know, in in the perfect world, we wouldn't need regulation because people would just do the right thing.  In some cases, though, yeah, people do need to be incentivised. | | |
|  |  | P4R2 |  | And and and I think is expected, people would if things go wrong, people would want to hope that there is a regulator there. | | |
|  |  | P4R2 |  | Well, the well standards are not typically not performed by government. Most of them are industry consensus. So they might be government people on on, on, on the committees of these things. But it won't just be government people. So it'll be considered. It'll be considered best practise. But the reason you need the regulators is because number one, I think in certain domains is expected. | | |
|  |  | P5R2 |  | Yeah. So if you skip down to the bottom question there, on the regulator or on the regulated sectors, I think that they do tend to pull back a little bit and they want the government to just tell them what to do because if they do the wrong thing, they're going to get slapped, right. And so I do think they tend to just wait for the government to tell them, you know, whatever the latest and greatest regulation is and respond to that, however.  I think in the last 10 years at least on the cybersecurity side of things, I think they are getting to be a little more proactive because they're understanding cybersecurity better. And again, this is a cybersecurity answer, not safety or anything else.  So it's just my experiences. Yeah, they they do a little bit on their own, but primarily they probably do wait for the regulator.  So that's that's why I just came a little bit somewhat agree. | | |
|  |  |
|  |  | P7R2 |  | Whatever. Whatever the frame. I mean, I'm. I'm speaking in general, so. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 190 of 316 |  |
|  | | | | | | |
|  |  | P7R2 |  | One way power you know? Yeah, yeah, yeah, yeah. | | |
|  |  | P7R2 |  | Right. So yes, it it, yeah, the we're beginning to understand this is a this is a a way of agreeing consents regulation isn't a way of an agreeing consensus rather than a one way. | | |
|  |  | P7R2 |  | So. So they're not they they are proactive. I mean they when they go to the regulator, they are ready sort of sort of speak. | | |
|  |  | P7R2 |  | And and that it it needs to come from them. And I think I think operators understand this. | | |
|  |  | P7R2 |  | I don't. Yeah, I'd say some would disagree here about about regulation because it's clear the regulators.  Communicate clearly to the to the licensees that they expect them to to essentially tell them how they conform whenever any. | | |
|  |  | P7R2 |  | Yeah, I mean the framework also.  Also helps in the sense that it tries to be not non prescriptive, but rather you know here is the qualities. Tell us how tell us what you're doing in order to conform. | | |
|  |  | P7R2 |  | You know, whatever is.  Safety or or security? You know the there isn't a specific sort of set of tick tick boxes that that that they go through but rather qualities if you like that then licensees have to say how they conform to. | | |
|  |  | P9R2 |  | They, they said, why don't I think about the regulation one, because I think regulation as you see when I get to the ranking of borders later, I think getting the regulatory environment right is actually really critical.  I think this is when I began to get this thought through what came up and became a stronger thought all the way through the report.  These things are true, but they don't have to be so.  And the thing about the regulatory piece is we can make it sort of broad statement that industry is very heavily driven by regulation, but.  Actually, industry has a really complicated relationship with regulation.  And we ought to draw some of that out. There are times when industry says we can see the right thing to do, but commercial practise will stop us doing it because the first one to do it will lose compared to everyone else. But we'd all be really happy if you'd regulate for it to happen. So we know we're on a level playing field hard to do internationally, but much easier to do nationally and therefore in the CNI space. So please, will you regulate to put us all on the same playing field so they will push for that because what they what they really want is stability.  Where I think the regulatory thing around CNI is really interesting is when we look at the financialization of the sector or of the various sectors, so Thames Water is being used as an example of this at the moment because it's in a particular pickle, but. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 191 of 316 |  |
|  | | | | | | |
|  |  | P9R2 |  | And there's lots of conflicting evidence about whether privatisation has led to increased investment or in infrastructure, or not in in the sectors, but it's generally felt that there hasn't been enough. And whereas there might be more than there was before, there certainly isn't enough to keep up with the demands on the systems.  But that's because meeting the demands on the systems is not in the interests of the shareholders.  That's irrelevant to the to to what they get in terms of dividends and when you look at the the driving factors of these companies, it is much more. How do you sweat the financial asset? | | |
|  |  |
|  |  | P9R2 |  | And they're caught in this systems loop of of saying, look, it's a critical national infrastructure. It will not be allowed to fail. Demand is utterly inelastic with respect to price. We can do what we want with this, knowing that the banks will lend us money on the back of it. We can take vast amounts of debt. Whether that debt gets invested in infrastructure. | | |
|  |  | P9R2 |  | And so we meet the elasticity that way and these sorts of organisations are open to ridiculous abuse. So we're seeing it with utility companies. We're seeing it with healthcare providers. We're seeing the social care providers and so on.  I think that is a much bigger driving force than regulation.  That's why I somewhat disagree. I think getting the regulatory environment is right. Part of that might well mean that CNI providers cannot respond to their shareholders over the needs of their customers. If you like, they need to be customer owned rather than shareholder owned for them to be able to meet the resilience objectives because resilience does not pay dividends. | | |
|  |  |
|  |  | P9R2 |  | Paid off in dividends and share buybacks is relent. Everybody else so we can do this and if it ever falls apart, it doesn't matter because the public will pick it back up again because they can't afford for it to fail because the demand is inelastic. So the price in terms of bills won't go up, but the price in terms of tax and public spending on it will. | | |
|  | | | | | | |
| **Only Respond to Regulation** |  | | | | | |
|
|  |  | P11 |  | the sense I got was that the industry was too much accustomed to kicking back and waiting for the regulators to tell it what to do.  And the regulator wasn't telling it to do anything on this, so it wasn't doing anything. | | |
|  |  | P3 |  | I you know, for stuff like machine learning, AI, autonomous operations, digital twins, you know, the the regulator at the moment doesn't really have the tools and methods to sort of determine whether you know actually what you're in, the evidence that you're providing is correct, right? | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 192 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Planning** |  | | | | | |
|
|  |  | P15 |  | If we're being really honest, it's what keeps me up at night. Is there aren't enough emergency planners doing things because there's not enough funding? Certainly.  I would say not necessarily in commercial entities because I don't know that so well, but the.  I would say it's a greater a sense of how.  How different organisations that are multi agency perspective are able to operate together.  So any kind of major instant response or major emergency or disaster response is never going to be just a single agency working on their own. | | |
|  |  |
|  |  | P15 |  | Aspect. So it depends on how depends on how that's being managed and how well they just how well they work together. And like a lot of it is, as ever basis on how people interact with each other. | | |
|  |  | P15 |  | So like what? What are the strategic priorities? What is it that we're even trying to achieve in terms of delivering a service and kind of what what is the minimum service required because effectively you're looking at for CNI, you're saying this is critical to the country to have these goods and not these services and provisions. And therefore it's basically essentially you're thinking about.  The UK as a as a as a business and doing business continuity.  But you need to know what the business's objectives are, what the business is trying to do, and I don't think that that I don't think those things are always clear.  And I don't think where they are.  Complicated industries with multiple different commercial interests. That blurs the line as well, and there isn't necessarily always a sort of don't really have a vested interest necessarily in sharing information.  About risks and how they're managing it, because that might also be a competitive. | | |
|  |  |
|  |  | P15 |  | Yeah | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 193 of 316 |  |
|  | | | | | | |
|  |  | P15 |  | And in the way that that was meant to happen, a lot of stuff during COVID didn't happen the way it was. As we are saying didn't happen the way it's meant to happen and that can be really so, which can be very shattering if you're like, OK, I've been provisionally working on these things for years and years and we've all been kind of kidding ourselves that when this happens, the exercises we've kind of gone along and said we'll all do X&Y&Z and then like, I'm, I'm not so naive as to think that everything would happen exactly as it does in the next class, because I think they're very fictitious.  Things, but I think they basically exercise is kind of help us kid ourselves that we are more prepared than we are and they don't necessarily reflect the reality of what's going to happen, which is in a major incident.  You're not only speaking to the nice emergency planner from service X in agency Y, who you know personally, but actually there's going to be like 56 other people in their organisation who you've never met before and who don't actually know anything about emergencies because they don't.  They like because it's not important enough for them. So I was at a Manchester Arena inquiry briefing the other day and one of the things that has come out of the inquiry, which you may or may not be aware of, is the.  Sorry, it's probably slightly tangential, but it kind of illustrates a point, which is that.  The police officer in charge of the police response from I think Greater Manchester Police, I don't think it was BTP.  Was unaware of what declaring Operation Plato meant, and somebody declared Operation Plato, or at least said that they thought it was, which is a marauding terrorist attack with a firearm. So they thought it was a firearms attack, not a bomb.  And therefore they've declared it because there is a particular arrangement of response that you do in that scenario to to manage it. And that is UK like that is across the UK. | | |
|  |  |
|  |  |
|  |  |
|  |  | P15 |  | Basic principles.  That you would also declare a major incident by providing a methane report, a basic principle that you provide an outline of what the major instant is, where it is, the type of incident, the hazards.  Numbers of casualties and so on. And some of these really basic things didn't happen because and those things worry me more, I think.  Which is probably not the answer that you're looking at, but I think we could do a lot better around some of the basic principles of Emergency Management. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 194 of 316 |  |
|  | | | | | | |
|  |  | P15 |  | They won't. They won't attend exercises, they won't attend meetings. They won't understand when when the big button gets pressed, that they have a role in it, like some of them are really good. Don't get me wrong, but like it, I found that extremely disconcerting. That's it. Like a really basic thing about what they were like. They had to go and look up what operation Plato was. And I was thinking.  They like a really senior police officer. How? How do they not? That's that is just so basic. I was absolutely staggered when I first heard that. So yeah, there are those things. But then if you're looking at again, if you're looking at risk management, there are the controls that you put in place in terms of preventative controls. So how do you, how do you stop the thing from happening in the 1st place? How do you reduce its likelihood? And then you're also looking at your responsive controls in terms of like the impact that it might have and and how well you deal with it because.  You you might address both of those, and you might still also have some residual risk leftover.  And therefore my my main concern, emergency management's main concern is on the responsive controls, but that's why it's really important and I think this is this probably is relevant.  In terms of like joining risk management up?  Risk management and Emergency Management together. So we've been doing some work in the rail industry that there's a whole load of risk managers who will manage everything like they will have risk management processes in place. They'll have asset management processes in place and change management and this and that and the other and there is a very poor interlinkage between what is happening there and the emergency plans. On the other hand, not and again, emergency planning and Emergency Management should be built around a really good understanding of, OK, what?  What risks are there about? How does that interact with the assets and processes that I we we are responsible for? What is my organisation even trying to achieve and what is the like risk environment that we're working in? What is our appetite for risk? Because if you're trying to run a train service, if you want zero risk, you can't run a train service like you can't run trains. So you have to accept there is some kind of risk that you want that that is tolerable.  Sort of set where where that is and understand it. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  | P15 |  | Not only you get people saying what are the risks? OK, we can look at the risks then you say, OK, well, what are the mitigations? Well, we can look at, you know, what you might do about it, and now you're saying, well, we can work out all the mitigations, but actually, that's not what'll happen in practise and.  Or you know, or or there's another step which is you've worked out what it is.  And then make sure that.  You're 50 big bosses who are too important to have to do all these exercises.  Exactly, yes.  Yeah, yeah. | | |
|  |  |
|  |  | P15 |  | And you then look at, OK, these are the risks, this is how it's impacting this is what we're doing, the OR these are the options of what we can do about it from a preventative and responsive nature.  That you can make sensible decisions around. Well, OK, We're happy to tolerate not doing much about it because we want to rely on our responsive controls. But we know that there is an inherent thing, and if that does go wrong, then we're liable to this. So you kind of understand what you're leaving yourself open to.  And at the moment, I think collectively and again, I can speak quite.  I can speak very articulately on the rail industry cause we've been doing a lot of this at the moment. Is that at a national level or a collect that collective understanding of risk doesn't exist.  There's and again, please do anonymize industries when you're talking about this, but like the collective understanding of risk, doesn't really exist. The like government steer on what they want the rail industry to do under certain scenarios, IE.  In COVID it was the same. They were not really clear about.  What they wanted the rail and St what to to do like, should they be protecting stuff and not doing anything? Should they be leaving the rail network open for freight because freight had a jolly old time? Because there are no very few passenger trains and therefore we were able to use the the rail network for moving.  Transporting other goods and services, which was really great for them. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 195 of 316 |  |
|  | | | | | | |
|  |  | P15 |  | And I think my kind of fears are we might have been in a good position X number of years ago.  But things are being like eroded quite a lot, and therefore people know stuff should be being done, but particularly in the health services and local authorities and and police and stuff, there aren't enough people doing it, even though they know and the people who are working there are are working under very different pressures. So I think it's probably those.  Like resourcing and funding kind of issues because they underpin literally everything that you're doing. It's all well and good saying I'm, I know I'm really worried about the situation in Ukraine, the impact that's having on fuel, the fact that we're like quite likely to have.  Major fuel issues if we have significant bounce of cold weather, we're going to run out of fuel and and we'll have issues around that. But like there.  They're sort of risk specific. I think I'm probably more worried about the more general context of.  How everybody works together in in a bigger sense, political direction in major incidents.  Which can be erratic at best.  And and their engagement in emergency response in advance of the incident. | | |
|  |  |
|  |  |
|  | | | | | | |
| **Poisoned AI Training Data** |  | | | | | |
|
|  |  | P14 |  | when you're dealing with how cybersecurity is going to be delivered by artificial intelligence.  Particularly if.  And this is another of the concerns being raised by the experts I speak to.  And then corrupt the learning data. So actually the machine's giving the wrong information. | | |
|  | | | | | | |
| **Political** |  | | | | | |
|
|  |  | P20 |  | I think it's possibly changing our political processes so we're less cowed and in Hock to these big powerful technology companies. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 196 of 316 |  |
|  | | | | | | |
|  |  | P20 |  | Umm well, you know, you look at what the E US done, GDPR, the EU AI act, fines.  Holding court, you know, companies to account with multi multi $1,000,000 lawsuits when they act irresponsibly. These are imperfect mechanisms and it that would take takes me into the whole fill of international regulation and governance. But you can do it if there's a political will. The EU have made some big steps in that regard.  I don't think there's any appetite in the current UK government to do it, because I think they're far too concerned about their mates in the corporate sector and and the millions that are being spent on lobbying and basically the corruption in our political system which prevents us actually doing something about corporate malfeasance in this area so.  Ultimately, I think it you know, as a political scientist, it requires political change. I think it requires stronger regulatory mechanisms it involves.  Corporate, you know, great growing corporate responsibility in the various ways and ways that we can do that involves it's a human resources challenge, as I said.  I think the the security by design trend is a is a good and important one. I'm a bit sceptical about whether it's going to really take hold as I've said, but I mean that's at least it's the right principle in my view.  And I think.  Yeah. I mean, it's a big question, isn't it? How can we, what do we need to do to better protect critical national infrastructure? I'm not sure I have the answer. I guess that's what what your your harvesting in terms of your project? | | |
|  |  |
|  |  |
|  |  |
|  | | | | | | |
| **Political Leadership** |  | | | | | |
|
|  |  | P10 |  | But I think it probably it should be, yeah, that sort of thing, you know, so I I just just something that's kind of Co ORDINATED doesn't have to be you know I'm I'm not I'm not you know I'm not I'm not overly invested or you know in my in my trust in in in the ability of the government to deliver on important things here shall we say you're my cynicism was clear when we started but I I think something like that would you know making it whole of society approach that's that's globally would like to kind of push on say bringing in industry you know people are throwing far more money on it in in business initiative than they are able to in government so.  What? What are they learning? What can they share?  Academia again, you know some some great minds and some great work, you know, get those people around the table rather than that, the fragmentation that we see at the moment, with everyone doing lots of, you know, a lot of busy work, how could we join this up and be more than some of our parts? I know that's a terrible cliche, but I kind of think this matters. | | |
|  |  |
|  |  |
|  |  | P10 |  | And so that that's that's, you know and and some very strong leadership and not getting quite so distracted by shiny things like AI. | | |
|  |  | P10 |  | Engaging, engaging here. Not not.  Not just focusing on the geopolitics, but, but you know they they obviously kind of setting setting the scene here. But I think you know some some real direction, some some.  You know, there is so many different agencies in in the UK in particular leading on this and then globally it becomes even more, you know, even messier. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 197 of 316 |  |
|  | | | | | | |
|  |  | P20 |  | you look at what the E US done, GDPR, the EU AI act, fines.  Holding court, you know, companies to account with multi multi $1,000,000 lawsuits when they act irresponsibly. These are imperfect mechanisms and it that would take takes me into the whole fill of international regulation and governance. But you can do it if there's a political will. The EU have made some big steps in that regard.  I don't think there's any appetite in the current UK government to do it, because I think they're far too concerned about their mates in the corporate sector and and the millions that are being spent on lobbying and basically the corruption in our political system which prevents us actually doing something about corporate malfeasance in this area so.  Ultimately, I think it you know, as a political scientist, it requires political change. I think it requires stronger regulatory mechanisms it involves.  Corporate, you know, great growing corporate responsibility in the various ways and ways that we can do that involves it's a human resources challenge, as I said. | | |
|  |  |
|  |  |
|  |  | P20 |  | I think it's possibly changing our political processes so we're less cowed and in Hock to these big powerful technology companies. | | |
|  |  | P21 |  | I think really changing the narrative that our privacy and our data protection that that's a risk to national security and to democracy and society as we know it. I think that that would be a thing for change. | | |
|  | | | | | | |
| **Poor Human Response to Incidents** |  | | | | | |
|
|  |  | P15 |  | if you look at the technological systems that support emergency services response and interoperability.  There are already challenges when it's working well because you're working with people who aren't necessarily like technically proficient in that way they aren't normally used to doing XY and Z, and this might not be at the forefront and therefore it's a sort of training and exercising and skills fade thing of OK, don't normally have to engage with this system very regularly, and I've forgotten how to use it. And now X has happened and the the plans that they need to do Y and I can't remember how to turn this thing on or I don't have the password like like you would be amazed how much like with the really basic stuff.  Goes wrong. | | |
|  |  |
|  |  | P24 |  | And we we were talking about this in terms of a critical infrastructure that.  We had digital tools. We should.  Give all the responsibility to them to monitor the operation of a telecoms network or the.  Health of a rich if there's the money turns. If there's a sensors in it doesn't say anything is going wrong, then why should I send someone to do the visual assessment? It's not required. I will have extra cost. Maybe if I do that.  And then the issue is trying to. | | |
|  |  |
|  |  | P24 |  | Like transfer these accountability to the tool, which is not actually accountable for that.  For trying to optimise things, but at the end of the day.  A human perspective and a assessment is always required. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 198 of 316 |  |
|  | | | | | | |
|  |  | P24 |  | You tend to forget how it worked before, so in general I I think that we forget how to do backup plans because we're very comfortable relying on a digital tools and maybe it's harder to cope with this disruptions now.  Because comfortable relying on.  This easygoing alternatives. | | |
|  | | | | | | |
| **Poor Incentives for Security** |  | | | | | |
|
|  |  | P20 |  | Bug bounties. Yeah, that they're sort of market market of, you know, will release this software which has lots of flaws in it. You find it for us and we'll pay, pay you for it. I just think it's it's it's quite bizarre really.  It's and and you know this whole the growth of this penetration testing industry for both software and hardware, you know, OK, we'll we'll build the digital network, we know it's not secure, but then we'll hire people come in to to come and test it for us.  You know, it seems to be security after the fact, doesn't it? | | |
|  |  |
|  |  | P20 |  | I guess I'm a bit sceptical about the extent to which that will change behaviour or people, you know, people will can be or companies can be incentivised to make their products secure by design. It appears to be a, you know, an initiative or a policy direction which.  Is set against some pretty big prevailing headwinds.  Because of the basic economics | | |
|  |  | P20 |  | I'm probably in the sort of more of the AI pessimist camp, I guess.  You know it will. It will and can have transformative effects. But but I think it's also fundamentally insecure, at least in in terms of how it's being designed and deployed at the moment.  And I yeah, I just. I'm sceptical that the commercial in commercial and political incentives will lead to responsible development. I mean the whole, you know, the whole thing is responsible AI, right? | | |
|  |  |
|  |  | P20 |  | If we learn the lessons from the last 1520 years of cybersecurity, I don't think cyber has been used very responsibly, so why would we expect it with with AI? So yeah, look, I am afraid I'm a bit of a pessimist. | | |
|  |  | P6 |  | Whatever crisis disasters in natural disasters.  It was out there a little bit, but it was never priority in no state we didn't spend.  Enough attention to it priority as societies all over Europe, I would call it. It was out there. Researchers were there, Ng OS were working there, but we didn't make it serious enough. And and the private market.  Did not invest in this kind of resilience because it was not necessary and that for me the solution when we come to the end, I think from a cyber security point of view, but also from this resilience point of view that our society is is still working, we need.  All together as end user private end user, | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 199 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Poor practice - poor quality - failure** |  | | | | | |
|
|  |  | P11 |  | It mean how deterministic is? We'll find out when my my my camera just freezes. I don't have the time to work out why. I'm sure that if I really did, I could. But in practical terms I won't and bring it back to the CNI. We're going to use the same technology. So how do we deter? How do we make it resilient in the face of a lack of determinism? That's essentially the point I'm making where you need to combine that top down and bottom up type approach to do the best of a bad job. | | |
|  |  | P11 |  | Right | | |
|  |  | P11 |  | Without any regard to likelihood or probability, what does a bad day at the plant look like? Well, we're going to focus our stuff on this and this and this, and we're going to use some, you know, we're going to divide it up into zones and we're going to try and make them sort of as as autonomous as possible. So we can, you know, all of that. And that's all good.  And that's based on a functional type top down.  Then with with the salute to Rasmussen and his thinking, there's a sort of bottom up type approach.  Which is asset based.  I would say that CIE is too much asset based. It goes too quickly to the systems and doesn't do enough of the functional decomposition. | | |
|  |  |
|  |  | P11 |  | But I would put it to you that we've got.  We've got to marry up both. You can't. You can't just come down from the top.  Because as I say, the sort of the the the stpa types and theoretic work assumes that you can do that and you can enumerate all your systems completely. You can you can effectively say your systems are.  Deterministic.  But I would put a parenthetical condition after that, which is only if they're sufficiently observable. Then you've got all the time in the universe. | | |
|  |  |
|  |  | P11 |  | But I do see there's Aus approach Aus mentality which is much more compliance based and asset based rather than functionally based and outcomes based. And if you you can see that also as an echo in their regulations the way that nirk nerk sip compares for example with the ONRSI apps in the nuclear environment where you you don't you don't sort of talk about.  That top down functional decomposition as much. | | |
|  |  | P11 |  | Well, I just around it and I just reject that model utterly. Now I think as we put the CNI of the future together or even deal with the legacy C and I, we already have, we're going to.  Have to adopt some of the more sort of system theoretic type stuff that Nancy Leveson talks about.  Except in a way that's practical. Sorry, Nancy. In a way that doesn't require more hours than there are in the universe to model the system.  And for the safety people.  Stop focusing on random.  Unrelated, uncoordinated.  Mechanical like, you know, like Poisson function type, you know. Oh, oh, here comes another one failures which we can model from historical behaviour. Where's all the system? Is it systemic? Systematic anyways.  Where are the systemic risks? | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 200 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | I | | |
|  |  | P11 |  | just in terms of let's call it artificial intelligence, let's even just call it machine learning, one of the rhetorical questions I think that.  And and bring it back to that digital twin for the for the weather forecast.  How do I determine the limits of my confidence in the outputs of the machine learning algorithm? | | |
|  |  | P11 |  | Exactly. Yes. The easiest. The easiest way to do the simple thing is to to bring in a massive operating system.  When I was talking earlier, I wasn't distinguishing between hard between hardware and software particularly, I did mention it a couple of times, but I wasn't. When I was talking about complexity.  I see the boundary between them being quite difficult to distinguish in terms of their contribution to to complexity, because for example the integrated circuit.  May have is it 2 billion transistors and has been has been laid out by a CAD Cam system that was written in C + + 20 years ago.  Or see or something. | | |
|  |  |
|  |  | P11 |  | OK, so that's so this is about. So we've got complexity in terms of hardware devices having maybe unnecessary, maybe just new connections, you know their own web servers and we have complexity in terms of I want to add 2 strings together. I'd better pull in Windows, you know sort of yes, yeah, yes. | | |
|  |  | P11 |  | Let | | |
|  |  | P11 |  | Let's put it more positively rather than pejoratively, to stand on the shoulders of predecessors in writing software. In other words, I will just incorporate this library. Well, it worked for me last year, so it'll work for me this year. Yeah. Where did it come from? I don't know. | | |
|  |  | P11 |  | Environments like Smrs will only be economically viable if they use technology that isn't currently regarded as being appropriate to those kinds of.  Safety critical environments, so you can't always get the sensors you want and the places you want. You can't always have individual wires going to every last sensor because there isn't the space and they're sealed for life.  So you end up having to do in make inferences to parameters rather than.  Bring them directly. May not be able to measure a particular pressure in a particular place. You may have to make some form of inference.  Using and here it comes using a digital twin.  And and so I see quite a lot now that's that's a sort of development beyond what I referred to earlier, which is that prognostication prognostics and diagnostics there we are.  The prognostics and diagnostics are effectively done, even if they may not be advertised as such against a digital twin.  And I think the question is. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 201 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | but I can't work out why I only mention it simply to say that not everybody agrees with me, but I believe that there is a relationship between the level of observability and the degree of determinism and.  In the system.  And you can't.  Ever achieve perfect observability?  Because there aren't enough days available to us or there aren't enough census or whatever. So to some degree you lack a. Your determinism reaches a kind of threshold and I use the example of something like a laptop or a or a Windows Server. | | |
|  |  |
|  |  | P11 |  | Since we're on digital twins, let me just make an observation in passing, there's.  Lyapunov there's there's some mathematics by Lyapunov. I'm told I'm not a mathematician.  Like a Lyapunov, I think coefficient which one can apply to to modelling like a digital twin which essentially.  So this is how it's explained to me by a mathematician. If I have billiard balls, I have some billiard balls. No, I want to calculate where the third bounce will go. Then it depends crucially on the angle of departure and the radius of the billiard ball. And there comes a point where I can't measure them sufficiently accurately such that I'm at a point of N it's just chaotic.  Well, you can regard that as being a good model for, for example, the weather forecasting system.  And the digital twin that's going to be running the SMR, that'll be just down the road from you, you know. | | |
|  |  |
|  |  |
|  |  | P11 |  | The way I see risk management being described and taught in different places is.  You can divide it.  This is a really messy subject and so I'm just going to tell you what I think rather than trying to explain and then I'll come back to where I see CIE in that framework.  If I take a standard like IAC 62443 which will be acquainted with it talks about having 2 levels of of risk management for for an industrial environment.  And I I like that, insofar as it goes, there are things I don't like. I'll come to in a minute, but I like it in the sense that it does what I would say is across the entire architecture, large hand, small maps. | | |
|  |  |
|  |  | P11 |  | Yes, yes. So even if you could have a perfect model and even perfect observations, et cetera, you couldn't get enough perfect observations to get true determinism. Yes.  Exactly. Of course you might. Yes, yes. | | |
|  |  | P11 |  | So. So you're you're thinking that actually a lot of the problems are going to come somewhere between all of these things. It's that going to be system wide types of problems rather than, yeah. | | |
|  |  | P11 |  | It's separate. So what it means is when I talk to.  And by the way, it's where I come from, so I'm hugely critical of the people who have, you know, that I've I work with.  What happens is the.  The safety engineers I work with abdicate responsibility, and if you read the safety standards and I'm I'm on a couple of committees and such like and I've reviewed one for railway, another one for nuclear, another one which is general, and they all suffer from the same problem as I see it, the safety standard says line one. Assume the security system is perfect and don't worry about it. | | |
|  |  |
|  |  | P11 |  | Yes and yes, and possibly emergent properties.  Which you don't actually see by investigating the individual nodes. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 202 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | Now | | |
|  |  | P11 |  | So I was asked recently what worried me about AI. And I said I thought that it would.  To greatest schisms in society.  A couple coupled with the way that people get their news because.  You end up losing trust in any source of truth.  And as soon as we get beyond a certain point, it's going to be very difficult to reverse the only basis of trust that I can conceive of is trust me, because I'm trustworthy. Because you know me.  And I think that this kind of fabrication of very plausible mistruths will lead to a world of each of us living in our own little echo Chamber of our own prejudices.  I think people are recognising that. | | |
|  |  |
|  |  | P11 |  | My concern, and by the way I I don't quite know how much of your interest is in the adversarial actions against the CNI and how much is just about wizzy technology for building the CNI. But I'm I'm more more concerned with the the adversarial action because that's where I come from. That is my, my history, my background.  I see security is being taught too much as an additive activity.  An existing system design.  Particularly one that has been through all the safety processes and has been deemed to be, you know, just just fantastic, that's just excellent. So now with your security nodes, please do whatever it is you do, but don't touch our system because it's, you know, because it's fine now we want to put it online. So we you'll probably want to put some do some stuff around it. | | |
|  |  |
|  |  | P11 |  | It's. Yeah. Well, it is a major issue, but it isn't yet resolved the other, so I'll just return to the point that I was going to make earlier because I was a little bit rude about my safety colleagues thinking that everything is about sort of random failures of pin joints with sheer bolts and things.  I think the problem I have with my security colleagues is that too much is about defending the network and the network attached assets to computer based systems. The software and you can actually have a conversation with.  Then for all forever for a day, and never once did they say. But what does this place actually do? | | |
|  |  |
|  |  | P11 |  | Oh well, since you are from the software background, I would share with you a completely different concern. I'll change tack completely. I think it's the way that we write software is a concern to me. It's.  I saw an article in the IEEE which I haven't read, but really resonated it said. Is this the year that we did finally deal with bloatware?  What it's talking about, I think, is the tendency to. | | |
|  |  | P11 |  | Nine shuttle, yes.  The IT it takes something like that to make people stop and say, well, how did this come? How did we come to this? I actually sent an e-mail to a colleague in NCSC saying something along these lines, like particularly the safety security thing. What causes me real anxiety is that at some point and I'll, I really will have retired by then. There will be the equivalent of the O rings or the OR the the Nimrod scandal.  And people will say.  How did we come to build industrial control systems in this manner?  Didn't we know? | | |
|  |  |
|  |  | P11 |  | Yeah | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 203 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | And then and that and and so you're saying in practical terms then that must mean that the models are too dependent on small fluctuations are likely to be quite dependent on small fluctuations. | | |
|  |  | P11 |  | He | | |
|  |  | P11 |  | Right. Well, that's a very interesting question because it takes us on to the next area, which I think you know you're talking about technology. I'd like to talk about. I think systems engineer, systems engineering issue, which is related to the use of technology because it's it's stems from that and the use of digital twins in safety critical environments.  You can also see it in the Purdue model, with vendors saying no, no, you don't need a separate card frame for this SIS.  The same controllers in the same car frame as the bpcs. It'll be fine. Don't worry, it's it's it's perfectly OK. Well, I'm not sure it is. | | |
|  |  |
|  |  | P11 |  | How do we know that this is going to wait?  How do we know that that digital twin is integrity is intact? | | |
|  |  | P11 |  | I feel less confident. I'm talking about this with authority, so I I don't really want to go too far down this road, but with the sense I got was that the industry was too much accustomed to kicking back and waiting for the regulators to tell it what to do.  And the regulator wasn't telling it to do anything on this, so it wasn't doing anything. | | |
|  |  | P11 |  | It's back to, it's back to that. It's back to that.  Functional top down decomposition. They're coming at it from the bottom up and they're coming up from from an asset based approach, and the clue is in the history historical title of of all of this stuff. But it used to be called network defence. | | |
|  |  | P15 |  | And | | |
|  |  | P15 |  | So for other, for the other incidents.  So there was a particular incident I'm thinking of that happen during COVID and I had spent a number of years working with that industry to develop part of the response.  And that response just completely did not happen. | | |
|  |  | P15 |  | And | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 204 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | Yep. So would that mean that will result in loss of function, wouldn't it? And and potentially permanent damage within within those systems so that recoverability is important you know.  And in terms of loss of function that goes back to.  What I was saying about functional safety, you know, don't don't put all your eggs in the AI basket.  That's be sensible about it and have a protection that says if AI does this then.  At least put a flag up and say, hang on, you know it's it's suggesting we do something ridiculous here and do something. So I. Yes, I agree with that, that statement. But I think the stuff that we can do well, there's there's approaches that, you know imply that you can recover from it or you can protect against it. | | |
|  |  |
|  |  | P20 |  | Bug bounties. Yeah, that they're sort of market market of, you know, will release this software which has lots of flaws in it. You find it for us and we'll pay, pay you for it. I just think it's it's it's quite bizarre really.  It's and and you know this whole the growth of this penetration testing industry for both software and hardware, you know, OK, we'll we'll build the digital network, we know it's not secure, but then we'll hire people come in to to come and test it for us.  You know, it seems to be security after the fact, doesn't it? | | |
|  |  |
|  |  | P20 |  | And you know, obviously you have this software secured by design narrative around software and and and hardware as well.  But you know I'm. I guess I'm a bit sceptical about the extent to which that will change behaviour or people, you know, people will can be or companies can be incentivised to make their products secure by design. It appears to be a, you know, an initiative or a policy direction which.  Is set against some pretty big prevailing headwinds.  Because of the basic economics, I don't know whether I answered your question at all there, Charles, but those are my random thoughts on software. | | |
|  |  |
|  |  | P20 |  | Well, so, So what? You're So what you're saying. Then if I understand is you don't see secure by design really working you you see.  Lots continued ransomware of various sorts and presumably improving in technology AI of all sorts you see.  Worsening political situation leading to.  Being used as a justification for arms race and for for bad basically bad software development, you know, seems bad justification to me, but but then yeah, yeah, that's what you're saying. | | |
|  |  |
|  |  | P20 |  | If we learn the lessons from the last 1520 years of cybersecurity, I don't think cyber has been used very responsibly, so why would we expect it with with AI? So yeah, look, I am afraid I'm a bit of a pessimist. I think, you know, obviously there are opportunities to to forge ahead and use AI to to enhance computer security. And there's just as much good work going on in that area, of course. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 205 of 316 |  |
|  | | | | | | |
|  |  | P20 |  | Yeah. I mean, what, what else? What else keeps me awake at night? Nothing, really. But I'm a pretty good sleeper. But.  Yeah, I mean I I think some of the stuff around.  I guess it's more academic at the moment and it's a bit more philosophical, but I'm interested in the emergence of General AI and Super intelligence and implications of that.  How quickly that might eventuate, whether that constitutes an existential threat? I mean, I think that what you know, the election stuff is this year this might be 2025, fifty years or never. But intellectually I find it interesting.  What kind of risks might the emergence of an artificial super intelligence create?  And particularly the idea that some people have commented on recently about irresponsible AI development processes, the idea that a catastrophe might be.  Something that could occur perhaps more easily in countries which aren't as transparent about their development processes. You know, we've just come out of this whole COVID pandemic where our ability to deal with COVID was severely affected, in my view, by a lack of Chinese transparency about what was going on. If we have a similar sort of scenario around AI.  Not transparent, you know, just as the Russians initially weren't transparent about the Chernobyl accident, how will that affect our ability to deal with the major crises in the area of cybersecurity or AI? So I think it's the election stuff I'm interested in longer term emergence of much more advanced forms of AI. And I think it's concerns around, again, how responsibly we're developing the technology and what I'm interested in doing research wise is really looking at the flip side, which is, you know. | | |
|  |  |
|  |  |
|  |  |
|  |  | P20 |  | And how and why do Actors Act irresponsibly when to point blip deploying technologies? And what can we learn?  From past cases of irresponsible technology deployment, some people in the management school doing some interesting work on that. But yeah, those are the sorts of issues that I think about.  In the technology space, obviously there's enough to worry about in the non technology space as well. In terms of more conflict and pandemics and and the situation in the Middle East and what have you. But those are the technological aspects that I'm interested in and think about quite a bit. | | |
|  |  |
|  |  | P4 |  | So this would, I guess be an example from space cause I I wouldn't call space or critical infrastructure, but I used to do some work in in that area, but I want once worked on a project I once worked on a team with with flight dynamics engineers and they were they they would write software for controlling the orbit and the attitude of of a spacecraft and they do it for all sorts of missions and they've they would they were very adept at writing requirements because they had to for other systems but they would they would they.  Would sometimes want services from other parts of the ground segment, specifically mission systems and the and because of the way the contracting stuff worked, it was always very hard for them to to get eddies sort of feedback.  So what they they developed this ability to write requirements knowing that they wouldn't be interpreted properly and knew that they would be able to if they wanted, they could take a strict interpretation of the performance of that particular requirement.  But such that when's the other people in the ground said and found out about it? | | |
|  |  |
|  |  |
|  |  | P4 |  | I mean I to fear I I'm I'm more concerned about poor quality.  I mean and anything which could happen as a result of that is is sort of unpredictable, but the unpredictability itself is not good, particularly with with software that needs to be certified, because if anything it's about certified certified certified software is based definition of deterministic.  There's all the bits of nondeterminism are removed. | | |
|  |  | P4 |  | They could say, well, you know, we we could relax that, but that other requirement over there that you said you couldn't address, you'd really need that to be done in order to sort of to sort of to sort of do that.  So it'd be very, very canny about. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 206 of 316 |  |
|  | | | | | | |
|  |  | P4 |  | I mean, if you imagine the sort of reason model of sort of you human error, the thing that actually killed someone or causes the causes harm is is it's often the tipper is a tip of a much bigger iceberg and the actual causes are are are well beneath beneath the service and and if you look at some of the Boeing stuff, some so that came out came out with the user there, you know you, you, you you basically had issues but fundamentally it was just bad.  It's just bad management and engineering practice because they're just trying to.  They're just because these folks are trying to cut costs.  I I I think a lot of a lot of issues that come to the news or come to the fore or get flagged and are not just in defense and others as well. | | |
|  |  |
|  |  | P4 |  | They were literally exploiting the fact that people were perhaps being ambiguous, but not realizing that they were being intentionally ambiguous with their sort of specs in order to bite some to to sort of buy some grease because the system changes in in, in in the future, it's not something, it's not something I've seen anywhere else.  Uh, But what I would say is that these people, I mean, I mean flight nomics folks have been writing software since since the mid 60s.  They are very.  I mean, I've I've literally written a paper about this.  My first ever academic paper was about requirements for, for, for.  For these sorts of people, they're very, very, very seasoned people at software engineering.  But even though they were preceded that as a sort of discipline, but yes. | | |
|  |  |
|  |  | P4 |  | Yeah, I mean I I have seen ambiguous.  I have seen discussions on contracts around certain things and is this partner doing this or doing that in my particular field?  But usually that's not malicious.  There's just people not reading things properly, but in this example, which is more, which is more scientific rather than commercial, it was literally intentional because these people that were so experienced at with with the software and the requirements and they had so many bad experiences that they literally were very defensive when, when, when their own specs. | | |
|  |  |
|  |  | P5 |  | Umm, there was three of us that are around the 2014, 2015 time frame were were sitting in a room together, working on a common project and we were we were just noticing that a lot of engineering firms, a lot of end user utilities operators, cause we were in the critical infrastructure mode at that time.  That everybody that we talked to, especially the engineering people, nobody had a clue about cyber security and that's only what nine or ten years ago, right? | | |
|  |  | P5 |  | You know, they're very localized.  Usually that don't propagate out somewhere because they catch it right away.  Somebody does, and so they correct it, but a malicious intent is far different than that.  They have campaigns that go to all kinds of things towards the end goal, whatever it is that they're wanting.  And so that's why typically we focus more on the malicious side of things and not just the random mistakes. | | |
|  |  |
|  |  | P5 |  | I I have nothing to prove this at all, but I'm guessing just from my experience that I've seen over many, many years that the incidental mistakes that people make type in the wrong whatever doesn't typically lend itself to catastrophic failures or consequences. | | |
|  |  | P6 |  | I don't believe that the AI community is at the moment addressing it. It's much more money spent on implement a little bit of new solution, do it and we are. It's working, it's working good enough. We can even sell it. But the important five to 10%, can I use it in a critical environment either from a privacy or ethical point of view.  Even can I use as I said in a safety environment, it's not helpful at all, and that's missing. Nobody organised it. I will send you an e-mail afterwards, yeah. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 207 of 316 |  |
|  | | | | | | |
|  |  | P8 |  | How to report something went wrong? How to follow up? How to make sure there's something done about it? Now training might be part of those solutions, but if the process is not in there.  For me to A to look if there is something going on when I notice something going on, if you don't give me a way of form to report it to note it down and then to follow up, I think the process is #1.  Training when the other thing when I see usability and so on. All I'm trying to say is the intuitiveness of the so any solution is sustainable if this, if the system is is.  Usable. This is sustainable solution if the processes are in place for me to notice, to get trained and everything. If it is part of the process is sustainable, we can follow up. One of training is not if it makes it so, yes, yeah. | | |
|  |  |
|  |  | P8 |  | It's a system problem, but Alice is fully automated, even if it's fully automated. Who designed it to be fully automated in the 1st place, and was it done right so because processes are done by humans, I link it to humans. You see what I mean? So the human fail, but it's not the human failure, it's the process failure. It's the system failing. Yeah, yeah. | | |
|  |  | P8 |  | Yeah | | |
|  |  | P8 |  | I I would say so. I mean the reason why I say this is because they say this in a lot of user interface experts. They say that UX and so on. So they have the fundamentals of the design but they apply the same sort of principles for almost every context because maybe they don't look for different pith matching ages.  Different personalities or different context. Even the Physiology of humans. Do you know, like the hormonal levels change? They may be focusing on one thing.  But human factors is is taken into account, so I think they say we study Physiology, we study psychology, we study.  Environmental science. We work with the pretty much of like an architects, so we are looking into how this light may be affecting you, not only the system. So anyway, I don't want to get too much deep into it, but it's a profession. It's a all the degree because it's located on. My fear is, if I will tell you that you can get trained, it will end up to something like some kind of fear. | | |
|  |  |
|  |  | P8 |  | It is a system wide problem, but depending on as well again that who designed the maintenance. So you need to look for the process maintenance process also done by humans. Maintenance systems are already taking care of you know or for example in railways now take caring 6 laptops. The bigs are hurting when they need to download the software. They may not do it because they are in pain. This sort of thing. So I can go on and on and on. It somehow links to humans. | | |
|  |  | P8 |  | Of the yeah. Of the failures of the failures, I mean. And when we say human, some sort of human, including maintenance. So for example. So there are one part the maintenance wasn't done right.  So so it could be different. So we didn't talk about maintenance. We talked about usability. There's also the maintenance aspect, which is also currently done by humans, not by robots at the moment. If the robots do it, you need to look for the main maintenance as well. So what we need to focus on focus on maintenance is well. | | |
|  |  |
|  |  | P8 |  | For equestrian, which they haven't defined, and that's what I find in cyber security. I mean it might be a bit of too much of a bold statement, but a lot of the cybersecurity engineers, I think.  Understand parts of the problem. They don't understand parts of the problem very well, but there's parts of the problem they don't understand very well and they don't put much of an effort to understand and human error is one of them. I think they have to put their focus on that. So that's my way. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 208 of 316 |  |
|  | | | | | | |
|  |  | P8 |  | So I mentioned the usability I mentioned like in other things, but these are all pretty much of like an underlying of try to understand the root cause. So to understand the root cause of either human error in a science that why the humans are falling for social engineering.  Is coming under. Why the human error have been stored? So what is the reason? I think all the efforts should be at this stage, at the very least.  To start, it should go there. Why human error is happening and underneath This is why are we falling for social engineering is due to our personality. Is it usability? Is it because the other guy is too sophisticated? There could be million reasons, but the question of why is that?  And really, pretty much when you try to like and understand the why, I would say.  Different discipline like the cross disciplines should really come together and pretty much.  So I can understand why this is happening, because you might be dead questions. A lot of mitigating strategies are being developed without really understanding why things are happening. So if you ask me where should we put our effort, I would say not. The question hasn't really answered yet. Everybody's finding a solution. | | |
|  |  |
|  |  |
|  |  | P8 |  | Sorry, I think I think it is for almost all systems, but then I say we need to understand why human error is happening because the systems are changing so fast. OK, now we are talking about P, domestic architectages and so on. So when you have an understanding of one part of technology, one part of system, this will change with the new systems. So for example, why human error is happening when we're using computers? If you think you answered this question, you haven't answered the question for though or Pete Mustiker artificial intelligence.  What I'm trying to say is pretty much of like your ongoing ongoing to try to understand with the with the technology, but it is a bit, it's it's not really catching up like in terms of the technology being developed, some sort of mitigation started being developed. But to really understand the root causes and actually to tailor solutions in my view not really catching up at the moment.  Somehow, because the black people are not in the same roommate by that night. | | |
|  |  |
|  |  | P8 |  | Where is it? Where you say people? You mean the users, isn't it? You don't talk about engineers, the users. OK, so, so the training is only one part of the story. So the so the people are not all trained this trip. However, the training is only one part of the story and it may not always be beneficial. The reason being because we get trained on one thing and the thing changes later on or we get trained in one thing.  Forget about it next month. So in terms of sustainability of the training is the problem. So therefore I cannot really provide the training as either A cause or a solution. So the so basically it is a part of the problem, but it is just a part of the problem. People put a lot of emphasis on it, but to be perfect owners, I think the processes are a bit missing in this game. Like if you are talking about, let's say nuclear reactor, different industries and so on, they should be a proper process.  In terms of how to notify like how to notice something went wrong? | | |
|  |  |
|  |  | P9 |  | I mean, you talk about the fact that the compute layer is now CNI, when it wasn't before and and a bizarre range of online services.  There is a there's a. There's a risk pattern emerging to come back to this adjacent possible idea, and the fact that innovation is connecting things together. People are building services on the back of really, really flaky previous services and then at some point it suddenly becomes desperately important and you realise that underneath it, you know, there's a fantastic XKCD cartoon where we say another one, lots of. Yeah, that's it. Yeah, that is it. That is it. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 209 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Poor Quality Software** |  | | | | | |
|
|  |  | P4 |  | I mean I to fear I I'm I'm more concerned about poor quality.  I mean and anything which could happen as a result of that is is sort of unpredictable, but the unpredictability itself is not good, particularly with with software that needs to be certified, because if anything it's about certified certified certified software is based definition of deterministic.  There's all the bits of nondeterminism are removed. | | |
|  | | | | | | |
| **Power Moving from Nations to Organisations** |  | | | | | |
|
|  |  | P6 |  | We asked them. Elon Musk is masked behaviour behind it. We see he is now partnered. He is part of providing and influencing even the the result of a war. Unbelievable. Just because he has a private infrastructure which he can provide or not provide. You see that's coming back to my first statement. Individuals are became already very powerful, which in my old days 10 years ago, we were just on the state level. | | |
|  | | | | | | |
| **Problems from Long Lifetimes** |  | | | | | |
|
|  |  | P11 |  | A disparity between the amortisation.  Expectations for a plant. Let's say I'm putting let's take something topical, like a a blast furnace. I'm going to put a blast furnace in in Port Talbot.  It's going to last 50 years.  Therefore, the control system will last 50 years, right? Well, wrong.  Because the nature of the technology on which it is based.  Has an assumed useful lifetime that is incompatible with the things that it's controlling anyway, it's that we can go on discussing it, but it's that fundamental problem that people aren't building in the expectation to either have to upgrade or replace the control systems. They hadn't, at least in the past. I think they're now getting hang of it.  But there's a heck of a lot of it out there already, and it'll still be there in 20 years time. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 210 of 316 |  |
|  | | | | | | |
|  |  | P17 |  | these OT systems typically have a life cycle of 30 to plus 60 years in some cases.  So, and they do tend to stay quite fragile and static in that time period. There will be minor changes. There might be a mid asset life upgrade on that system. So because of those time scales and because of you know, just actually by us humans, you know changes, employment skills, you know lots of information.  Commercial aspects. The information about those systems tends to get lost, and it it there's a lack of understanding | | |
|  |  |
|  |  | P4 |  | When you say create the software, I mean we we're not just talking to people that are developing the software, we're talking about people that are gonna be evolving it, maintaining it.  I mean, we're talking about a plan.  We're talking about platforms here that will be around for maybe four or five decades, which actually and if you look at a lot of critical infrastructure, these are long lived systems. | | |
|  |  |
|  |  | P4 |  | we're gonna one of the requirements we've actually put in is this is gonna have to run for several decades.  And how are you going to make sure that that knowledge is sustained over that period? | | |
|  | | | | | | |
| **Quantum Cracking Crypto** |  | | | | | |
|
|  |  | P13 |  | just kind of the cyber security arms races.  Where somebody cracks or has a quantum computer, they can crack.  Cryptographic systems we rely on today are they instantly changes everything, doesn't it? | | |
|  |  | P14 |  | Which aspects of the of the threat the the only limited issues I can identify around threat is simply that it gives the the ability of I say bad actors and of course.  What we might be talking about is the democratisation of.  Weapons and tools so that bad actors can decrypt.  Encrypted data and get in and penetrate and do weird and wonderful things to the critical national infrastructure. | | |
|  |  | P14 |  | On the quantum side, clearly.  Just the massive game changing potential of quantum computing.  Could have extraordinary impact and threat. | | |
|  |  | P16 |  | As humans we we are not. We are not used to process information over 50 years for us. It's like, you know, we live in the present and and it's a good I think it's a good thing. It's an evolutionary thing. You know we we need to survive the present not in 50 years from now when most of us will probably be in a very different place. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 211 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | So, so because I don't know if you've seen those presentations where the people say like the quantum people say, well, when encryption is gonna be brought universally broken by a quantum.  Computer all the secrets that have been collected over the past decades, they gonna instantly become.  Transparent to anyone and then people will use AI to kind of craft.  An understanding of the present based on past transactions and past.  Communications. So we need to now protect or.  For a future.  For a quantum future, and there are some existing mathematical and ways to do it without quantum technologies. But even if it's discovered in 30 years from now, we have to protect secrets now.  If these secrets need to be maintained for 50 years, for example. | | |
|  |  |
|  |  | P16 |  | in Canada, we have A and I'm sure I think you also have that in the UK, but a very strong quantum computing.  Community and I think that if we are looking a bit further in the horizon, I think 10 to 25 years ahead. I think the quantum threat will probably be something that will also be very, very disruptive. And as you know, that's something that we should pay attention right now. But it's so far in the future and so unpredictable.  'Cause no one knows exactly when someone is gonna be able to.  To harness quantum computing to break all the all the encryption. So it's very for companies that are facing on a daily basis the constant barrage of conventional cyberattacks and then now AI powered cyberattacks. The quantum threat is like something that just doesn't register because they just have no bandwidth left. | | |
|  |  |
|  |  | P21 |  | So the one of the other papers that we published on this was on the the harms that result as a consequence of ransomware attack. And this is ransomware, but it could also be other encryption or intrusion based crime. So it could be broader than that.  And in our research, there was no indication that some of the data that's been harvested by cyber criminals and leaked on the dark net, there's.  Additional harm resulting as a consequence of that because.  Criminals might use that data for further criminal activities. | | |
|  |  |
|  |  | P21 |  | So not the past, who's actually suffered the ransomware attack by the person who whose data has been leaked. And all of us by now will have gotten emails from capital. I don't know whom, that our pension date has for leaders of health. I think it could could expand the notion of who's a victim. And then in turn, those who've previously been indirect victims, they could be turned to direct victims because they might then face crime fraud or something else.  As a result. So that would mean psychological, financial, reputational harm on them again. So it's really expands the the notion of who can be a victim. | | |
|  |  |
|  |  | P21 |  | I mean, quantum is sort of sort of always there. | | |
|  |  | P21 |  | But one could imagine a scenario where this, perhaps less on a criminal spectrum, more in an espionage spectrum where they're harvesting data that is encrypted.  They currently can't access, but in retrospect they might be able to access that by 2040 because by then they have the capability to decrypt. | | |
|  |  | P21 |  | Or perhaps also the ability to, in retrospect, in retrospect, decrypt some of the data that's been harvested. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 212 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | This is by the darknet, but also commercially available data. I think it's quite.  Daunting at times, how much data is out there? We don't. We don't quite grasp, but particularly how much information that data.  Turns into if you overlap certain data sets.  And I think that our ability to really.  Use. The data will increase because at some point it will be more about the quality of the data rather than the quantity, and I suspect there may forthcoming technologies will enable us to to sort of make use of equality alternative to something qualitative rather than just relying on on everything that's publicly out there right now. | | |
|  |  |
|  |  | P21 |  | But I also think.  Industrial espionage, perhaps. | | |
|  |  | P21 |  | that if I'm a lawyer, I've suffered from lansomer attack and my my clients data has put on the dark net. They are then exorted and they become subject to further crime because of that. | | |
|  |  | P21 |  | , you can also can also be less sophisticated, right? I mean, a lot of what we're seeing in this context isn't actually as sophisticated as as something like that. But by 2040, who knows? I mean, cyber criminals have been pretty inventive and pretty have welcomed new technologies with open arms to ensure that the business remains lucrative. | | |
|  |  | P21 |  | I think the number one game changer I would see is.  If more of the the data that we've seen stolen for in ransomware attacks and other intrusion based crime or espionage, for example, if there was either ability to decrypt some of our data very respectively, or just analyse some of the unencrypted data that's been harvested, I think that would quite fundamentally change the ecosystem in which we in which I sort of look, I sort of look at in terms of.  Cyber crime.  Policy making. | | |
|  |  |
|  |  | P23 |  | if someone builds a performance quantum computer, there will be really diabolical attacks that one can make.  Umm, what we describe as the idea that of of not attacking an individual computer, but using one's resources to attack a software signing certificate or a website certificate.  And then all you have to do is get someone to visit that website or download the Microsoft update.  That would be that would be the attack right now.  We'll just, Steven, assuming that one had a quantum computer that would be a very, very, very expensive attack on on the order of millions of dollars. | | |
|  |  |
|  |  | P6 |  | Yeah, there is potential threats from a quantum computing point of view for the encryption. I think this thread is serious. There's a lot of money is implement and a lot of sponsors are there to build such quantum computers. It's not yet there, but I imagine that this will be feasible. Human beings can do it. So we have a quantum computer there and then.  Lousy existing asymmetric encryption is under threat, and since the whole world is based on this, this threat is there. I see it very serious. We had. I mean, I'm also active in there. I'm biassed OK, but I think we have to think about it. How can we build next generation encryption just because it could not be that the whole world can read our data exchange, so we have to find means plus quantum encryption QKD. There are technologies out there? Which technology?  Finally, will be the successor in the global market.  See Market will define but activities are going on. I see differences also between Asia, Europe and us on panic resolutions on this. So this threat on encryption is there.  And then you mentioned when I come to cybersecurity, I think. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 213 of 316 |  |
|  | | | | | | |
|  |  | P7 |  | So I think that's the that's potentially a very big problem for for all sorts of sectors and it's and it's similar to you know potentially quantum computing that might be the other technology that's down your list, right, can can can be used for good, can be used for, for for bad to, you know, weaponize an adversary. | | |
|  |  | P9 |  | But you also really, really do want it to be secure, | | |
|  |  | P9 |  | We've got interesting conversation with somebody about Central bank, digital currencies and whether they need to be secure against quantum crypt attacks. And the challenge of course there is in a cryptocurrency or processing time is your transaction time. So you don't really want it to be very secure because that costs a lot of compute. | | |
|  | | | | | | |
| **Quantum Decryption** |  | | | | | |
|
|  |  | P16 |  | for Quantum, I think that's. | | |
|  |  | P16 |  | Probably startups trying to help raise awareness and prepare.  Critical infrastructures to the to the possible event of no encryption. You know, all encryption being broken down, but I think not all critical infrastructures are not going to be affected the same way. So financial institutions for them, I think it's a big it's a big issue to preserve the confidentiality.  Older transactions.  Future and past and future.  People infrastructure | | |
|  |  |
|  |  | P16 |  | in the in the food supply chain, I don't. It's going to make any difference. I think they have many bigger fish to fry or they have many other issues. You know whether missions have been broken. I don't think they're going to care that much. I mean, it's not going to be their top three priorities. So I think it's going to be very different in terms of impact, I think the.  The critical infrastructure is dealing in information and needing to preserve the secrecy or confidentiality they got to be very.  Effective and they're going to probably be more.  Buying and thinking about how to embed quantum quantum proof systems and technologies into their systems. Others they will just say no too, too too complicated. What's the what's the use for us? So I think that it's going to be more diffused. | | |
|  |  |
|  |  | P4 |  | in security and safety issues of autonomous systems.  If you look at what people in the lab are up to, you'll hear lots of talk of quantum, so lots of lots of interest around that.  What other things? | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 214 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Quantum Resistant Encryption** |  | | | | | |
|
|  |  | P23 |  | And the and the good news is, is that many actors are creating quantum resistant infrastructures.  So I I do think we have runway to fix to fix some of that. | | |
|  | | | | | | |
| **Rating Vulnerabilities in Terms of Human Contributed Impact** |  | | | | | |
|
|  |  | P12 |  | Identify critical vulnerabilities or like things that have a high C of ESS score. But again, some of the things that matter most don't necessarily have acvs score, right, like calling up someone and being like, hey, I'm so and so can you please XYZ?  That's not covered by CBSS scores, and of course, AI does make those attacks easier right deepaks of whatever, which brings us back to the like. We need some kind of cryptographic scheme to to authenticate, but yeah, yeah. | | |
|  |  | P12 |  | And, you know, this goes back again, so many of these things are social issues. But, you know, just like responsible disclosure stuff is really hard and, you know.  Yeah. Like, I think identifying vulnerabilities isn't assigning them acvs score like that loop should be improved tremendously by AI. So I'm actually that's one thing where I'm optimistic in aggregate that it will actually help people. | | |
|  | | | | | | |
| **Regulation to Incentivise Risk Management** |  | | | | | |
|
|  |  | P3 |  | You know, do we have the right regulation? | | |
|  |  | P3 |  | That incentivizes all of this, you know. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 215 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | Those vulnerabilities in our great infrastructures that we have very complex systems. So in Europe, we are answering now with increasing regulation and laws like NIST two and the Resilience Act. I think I believe it's a, it's a huge burden on the manufacturers and suppliers.  But I believe it's necessary that it's done, otherwise we will end up in a big mess | | |
|  |  | P7 |  | OK, let's assume we solve this all these problems from a technology point of view, right?  How are we gonna? How are we gonna get the companies and and then the critical infrastructure providers to run any of these on their on their systems, what do we need to do?  We obviously need to get it somehow certified. We need to get it regulated. We need to get the operators to understand an interface with it, which is one of the questions you alluded to.  Elsewhere. So this kind of I think ecosystem organisational integration, I think it's it's it's also very important and it's at the end of the day, I think it's the, it's what it will make the difference from having nice scientific papers about something versus having something deployed in on on real systems. | | |
|  |  |
|  | | | | | | |
| **Research into Human Errors** |  | | | | | |
|
|  |  | P8 |  | Say human factors is pretty much is a profession like in itself. So to be able to do this job and other people are focusing on UX but essentially looking into the task of the user that you need to understand how to the whole task analysis for example you need to understand to look into like an environment you need to look into the humans, the skills and capability which is part of psychology and cognitive psychology. You need to look into Physiology. You need to look at all the other things. So yes. But what I'm trying to say that if I understood the right I mean.  It's around, but it's more sounds like for example, I'm asking you, can you trade me on cybersecurity? You could be, but then you have to understand the whole.  Topic behind so that's why I guess what I wanted to say was that more like cooperation between him, in fact with professionals for the psychologists and the cybersecurity engine, if I understood that if we just train, you will be seeing one part of it. So if we can tell you, look, make this system more simple. However, this context dependent again, you may be able to consider in one context if you train you for it, but if you don't understand the wider.  Fundamentals philosophy behind it, you may not be able to understand it. For example, in a nuclear reactor because you will not be looking for the things that we are looking for. Does it make sense? | | |
|  |  |
|  |  |
|  |  | P8 |  | So they have the fundamentals of the design but they apply the same sort of principles for almost every context because maybe they don't look for different pith matching ages.  Different personalities or different context. Even the Physiology of humans. Do you know, like the hormonal levels change? They may be focusing on one thing.  But human factors is is taken into account, so I think they say we study Physiology, we study psychology, we study.  Environmental science. We work with the pretty much of like an architects, so we are looking into how this light may be affecting you, not only the system. So anyway, I don't want to get too much deep into it, but it's a profession. It's a all the degree because it's located on. My fear is, if I will tell you that you can get trained, it will end up to something like some kind of fear. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 216 of 316 |  |
|  | | | | | | |
|  |  | P8 |  | I think all the efforts should be at this stage, at the very least.  To start, it should go there. Why human error is happening and underneath This is why are we falling for social engineering is due to our personality. Is it usability? Is it because the other guy is too sophisticated? There could be million reasons, but the question of why is that?  And really, pretty much when you try to like and understand the why, I would say.  Different discipline like the cross disciplines should really come together and pretty much.  So I can understand why this is happening, because you might be dead questions. A lot of mitigating strategies are being developed without really understanding why things are happening. So if you ask me where should we put our effort, I would say not. The question hasn't really answered yet. | | |
|  |  |
|  | | | | | | |
| **Research into Trust and AI** |  | | | | | |
|
|  |  | P14 |  | from that point of view, I would argue that builds resilience, so. | | |
|  |  | P14 |  | there's a big.  Ukri programme, I think it's 30 million gone into it around trust and AI, which people are worrying about. | | |
|  |  | P6 |  | Functioning of the system without bias and could conform. So how can we test and verify and validate AE algorithms? So that's also a new research field which started I think 10 years ago which started 10 years ago.  It's not mature at all. We need competence all over the world. So the question is, are we able from mechanically point, if you're really to master the EI technology by this mean, not just applying them, that's everybody's doing, that's easy.  But I'm asking exactly. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 217 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Resilience** |  | | | | | |
|
|  |  | P19 |  | Scientific and technological cooperation in Europe.  You gonna try to.  This course actions create communities as well as contributing new new thinking to technologies.  So this is a resilient community, right to create this?  On the the cost action, I think I I think is an example of how you you might collect people together and and to come up with ideas.  So you know, for many, many different directions.  So yes, he could when you could build up the the discipline of resilience.  It has been. | | |
|  |  |
|  |  | P19 |  | So I became interested in.  Security to some extent, that's not data security so much your system security and it moved on about 15 plus years ago to resilience, which is the ability of assistant to continue to provide the level of the quality of service that promises even in the face of adversities, challenges of all sorts.  So the word challenge became important for for me and my work.  And it's not just cyber challenges.  It's what happens anyway with with normal computer systems overloading for example, and then of course malicious attacks, physical attacks, even just typical faults and failures that happen.  And I discovered that and xxx Systems certainly hadn't been properly prepared for resilience and challenges in the future. | | |
|  |  |
|  |  | P19 |  | No, there there's a there's a.  There's a tech thinking about technical book.  xxx  Yeah, that was the theme of this course of action. | | |
|  |  |
|  |  | P19 |  | Resilience has been been around for four years.  I somehow, along with Service safety that thinking, but I think it's it it no needs to to become a topic in its own right.  And presumably it starts with risk assessment and yeah, moves through, yes.  And the and.  If you look at some of the material, for example in the.  In the look I did it with Yasid right and that will give you see that the right a number of different approaches right to to building resilience systems and they they all more or less have the same definition of resilience.  Only the the exact wording is is not as important as it's actually doing something about yes, yes, and make making life better for everyone is as a result of yes, yes, that kind of work. | | |
|  |  |
|  |  | P19 |  | So Paul cost action.  Cost has been a is a European program that's been going for a long time.  OK, right. It says. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 218 of 316 |  |
|  | | | | | | |
|  |  | P19 |  | Probably companies that are are designing systems instructs probably do some of the there's already yes, because they they have forums where they talk to users and they they tried to build the they tried to specify the software so that it will six.  You know what?  The users need what I'm saying is alongside of that, the you you have to think about the risks of things that will go wrong.  Probably you, you you know, you're you're deciding how much redundance you're redundancy to to fit into the technical parts of systems.  You have to think about how you you deal with the the likelihood of people be compromised or people making mistakes. | | |
|  |  |
|  |  | P19 |  | I I you you mentioned about your technologies, you you mentioned about quantum and yes, yes, you mentioned about about AI.  I don't know whether these these kind of systems we'll introduce more vulnerabilities.  I I don't know whether that be more or less difficult to yeah, to make resilient but but the license still holds.  Think Brazilians, if you if you want to build systems they they have to have certain properties.  And I think the high availability and reliability. | | |
|  |  |
|  |  | P19 |  | Plus something of the the attributes of these both need to be to be assured. Especially no.  Yeah, no resilience that availability and reliability are are statistical figures.  Yeah, you you can't have package systems that you.  You need to make them fit enough for purpose to invest enough to make sure that the probably are.  Yes, I don't.  And of course, our cybersecurity colleagues are right.  They're working away on on how you make combat the the the attacks that yes that you have.  But I think some of them don't probably don't go far enough that that begun to talk about cyber resilience. | | |
|  |  |
|  |  | P19 |  | Where do you think we should be putting our effort to address and prevent them and effectively you've been saying that we should be working on resilience of various sorts and not worrying.  Obviously we try and prevent them done.  It's it's resilience that we care about it.  Yes, yes, we're still don't tell the building and the capability to detect problems happening to act fast, to recover it and that recovery and the recovery getting back to to normal services is very important. | | |
|  |  |
|  |  | P19 |  | How how do we?  How do we coped with this?  Given that these systems are not not not that well protected, but the moment Charles, I think that more research is needed in the field to to, to design and and actually to after the fact.  I resilience into systems, could you?  You can't just start again and and and they'll just look from scratch.  So I think it's important to to use people, people from other disciplines to think about the the risks involved in no resilience comes at a cost, because with resilience, we're talking about adding redundant components and paths.  So the the these are are gonna cost and I I suspect that in the past systems and service providers have maybe been a bit reluctant to to add.  Yeah, costly resources like this, of course. | | |
|  |  |
|  |  | P19 |  | Now I I mentioned about RTI and about organizations and people.  Working with people from other disciplines is really important in this because the source of many problems comes not not just from the technology, but actually more from the people.  Yes, if if you if you get side successful cyber taxes, it's often the case that the someones been engineer.  Human engineer.  Yeah, there may be malicious insiders.  They make you will be familiar.  Yes, kind of thing that's upset.  How how do we deal with this? | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 219 of 316 |  |
|  | | | | | | |
|  |  | P19 |  | Of course. Yeah.  I mean, and again, there may be people that will usually be people involved who don't get reported incident that might be an electronic signal that comes up and they'll say we we can see that there's a the component has tripped and then they they will have redundant equipment to.  Yeah, to to plug it in and and to work on and then they'll send it engineers out to prepare the field unit or whatever.  No, they they have the they have that kind of will handle but that that that is relatively easy compared to some of the these more complex systems which software systems which may be subjected to.  To tax of a different sort or yes, or accidents of a different sort.  And where, of course, the traditional industry experts are not trained to know about problems in software.  You know how there's been a lot discussion about the post office standalone recent times it's it's it's it seems remarkable that that many, many people, not least for postmasters themselves, didn't know, didn't seem to know that computer systems can go wrong indeed. | | |
|  |  |
|  |  |
|  |  |
|  |  | P19 |  | I'm what when I a few years ago in a European project, I started looking at with others the how, how you would add renewable sources of energy into the the traditional power systems.  And it's a it's it's amazingly complicated and it's not.  It's it's not as I thought.  Very easy to keep these systems stable.  Track it never was.  It's a better, better of an illusion, actually.  And and so actually the the this the struggle to to make computer networks in Tyler resilient is pretty complex and I think that we we need to perhaps to learn lessons from from other utilities if if that is if they've looked at how how how you need to make please systems entirely dependable.  And and of course in in, in in power systems it was relatively easy when there was a big power station and just yeah, tree that delivers. | | |
|  |  |
|  |  |
|  |  | P19 |  | You using Tonkin and machine learning systems?  I don't like using the word.  Terry I but but but some kind of.  Trained systems data process which are quite quite complicated these systems themselves.  I think the introduced more vulnerabilities than than you might imagine, so it's even more important to think about resilience by design.  So I any kind of any kind of system that that could be part of the critical national infrastructure needs to be designed to resilience in mind to think resilience and and in fact some of the stuff that I've written in recent years has been to try and get this message across. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 220 of 316 |  |
|  | | | | | | |
|  |  | P19 |  | Down, down, down, down to to to the users.  It's, well, actively easy.  I supposed to keep that stable, but even that's got its challenges now.  Now that the they're adding in renewables that they they have to think about about what we're thinking about, which is when when you have faults, failures, attacks, cyber attacks included that that will that will challenge and jeopardize the operation of these systems.  They they know it's important.  I sometimes worry that that the the people who are pick computer networks don't really realize the problems.  Now, in recent time, do you ask about about modern technologies?  So computer networks are. | | |
|  |  |
|  |  | P19 |  | And I think that that's important because I think some folks in the past have thought if if we if we build enough protection into systems.  Yeah, well, there.  But they were all right.  But you have to think about what happens when the world gets benefited.  Yes, you have to to think about the perhaps unlikely, but all too frequent penetrating of the cyber war.  What happens when the bad guys get in?  Yes, you've got to be prepared for that.  And that's about. | | |
|  |  |
|  |  | P19 |  | In academic terms, telecoms tends to be done in electrical engineering department, so they do the physical layer stuff and you know the the the latest generations of wireless systems, for example 5G, it current one and the looking to to make he systems even work physically capable and in the future.  But of course, what I'm interested in is that the layers above the physical systems are layers is on, call them, and then you have to face with users, yes, and.  One thing I should mention is that it's not just technology that's involved in in the need for providing resiliencies.  It's also organizational issues on people issues and I know what we've begun to rock some years ago to talk about what TI organizations, technologies and individuals. | | |
|  |  |
|  |  | P21 |  | It's no, it's very it. What is what? What we it is fascinating to see all the way around the problem. So we started off we we started off just sort of thinking.  Who? You know, how might people do bad things to critical infrastructure? And it's gradually becoming clear that that's not really a very interesting question. I mean, obviously there's lots of, you know, if we can stop them doing it, that's great. But really it's how are we going to survive it when it happens.  What makes us resilient? What? And and also what sort of effects that has and and looking at this from every and you know you're you're from the point of view if it's happened and who are the victims and stuff that's really interesting. | | |
|  |  |
|  |  | P22 |  | So we spend a lot of time, you know, changing people's vocabulary in the BCS, who think that software resilience is the same as service resilience. Service resilience is about lost user hours, software resilience in terms of the ability of a software component to recover. Both are important. If you start with the lost user hours, you can then start homing in on where to improve the software resilience of component. | | |
|  |  | P23 |  | I mean, like people suffered it, you know, you have your power turned off and people suffer.  I'm and there's a.  There's a recent attack where essentially the same thing happened.  Critical infrastructure attacked it could operate, but it decided to shut down.  So we need a legal innovation that gets critical infrastructures to the place where, if they can operate, they do and I don't know what that is.  I don't like as far as Colonial pipeline went like, why couldn't they just build people after the fact?  I mean, do you ultimately have meters? | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 221 of 316 |  |
|  | | | | | | |
|  |  | P23 |  | Well, on the on, on the legal side, one of the, so just purely legal side, one of the goals that we haven't been able to quite reach yet is the idea of resilience.  So, umm, the colonial pipeline attack in the US is a great example where.  Colonial actually could operate its pipeline, but they shut it off because they couldn't bill.  And so, like, people froze. | | |
|  |  | P23 |  | Yeah, well, that's what I actually, no, I I have talked a lot about technology problems in law was what I wanted to what I wanted to talk about because because because that's your speciality.  But, but also because it is important they it is very important and it's and.  Certainly in the addressing of these, we've come across the need for resilience, but again, to have resilience is a human.  You know, as got to involve the humans involved, the humans there.  And again for that you need to have the law and the legislation and the, you know, what the sorts of things you've talked about are exactly the solutions to that sort of resilience.  So I'm I am.  I'm delighted you are speaking about humans.  That's what humans and law, because this is very valuable. | | |
|  |  |
|  | | | | | | |
| **Risk and Emergency Management Skills** |  | | | | | |
|
|  |  | P14 |  | is the House of Lords. Did a study on this three or four years ago and was identifying that there are serious failings in terms of the capacity and the capability of the country to do good risk management. And that for me is a big issue. | | |
|  |  | P15 |  | what keeps me up at night. Is there aren't enough emergency planners doing things because there's not enough funding? Certainly.  I would say not necessarily in commercial entities because I don't know that so well, but the.  I would say it's a greater a sense of how.  How different organisations that are multi agency perspective are able to operate together.  So any kind of major instant response or major emergency or disaster response is never going to be just a single agency working on their own. | | |
|  |  |
|  |  | P15 |  | So we've been doing some work in the rail industry that there's a whole load of risk managers who will manage everything like they will have risk management processes in place. They'll have asset management processes in place and change management and this and that and the other and there is a very poor interlinkage between what is happening there and the emergency plans. On the other hand, not and again, emergency planning and Emergency Management should be built around a really good understanding of, OK, what?  What risks are there about? How does that interact with the assets and processes that I we we are responsible for? What is my organisation even trying to achieve and what is the like risk environment that we're working in? What is our appetite for risk? Because if you're trying to run a train service, if you want zero risk, you can't run a train service like you can't run trains. So you have to accept there is some kind of risk that you want that that is tolerable.  Sort of set where where that is and understand it. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 222 of 316 |  |
|  | | | | | | |
|  |  | P15 |  | So I think there are but within that at the same time it's it's had to be more smart because there's hardly any resources for.  What's going on? So where teams might have had, I don't know. Hypothetically, there might have been a team of 10 in 2000 and eight 2011 on the run up to the Olympics in London. Teams were very well resourced. And then after that it's just been steadily eroded. And therefore, you're working with much smaller numbers of people.  And I think that that is not a dissimilar situation from two other count one and two responders where people are double hatting.  I don't know how you solve that necessarily, other than magically coming up with some more funding that wouldn't otherwise go to the NHS for day-to-day service provision and schools and education and all the other things that we need money for. | | |
|  |  |
|  |  | P15 |  | They won't attend exercises, they won't attend meetings. They won't understand when when the big button gets pressed, that they have a role in it, like some of them are really good. Don't get me wrong, but like it, I found that extremely disconcerting. That's it. Like a really basic thing about what they were like. They had to go and look up what operation Plato was. And I was thinking.  They like a really senior police officer. How? How do they not? That's that is just so basic. I was absolutely staggered when I first heard that. So yeah, there are those things. | | |
|  |  |
|  |  | P15 |  | You're 50 big bosses who are too important to have to do all these exercises. | | |
|  |  | P15 |  | I can speak very articulately on the rail industry cause we've been doing a lot of this at the moment. Is that at a national level or a collect that collective understanding of risk doesn't exist.  There's and again, please do anonymize industries when you're talking about this, but like the collective understanding of risk, doesn't really exist. The like government steer on what they want the rail industry to do under certain scenarios | | |
|  |  | P15 |  | And I think my kind of fears are we might have been in a good position X number of years ago.  But things are being like eroded quite a lot, and therefore people know stuff should be being done, but particularly in the health services and local authorities and and police and stuff, there aren't enough people doing it, even though they know and the people who are working there are are working under very different pressures. So I think it's probably those.  Like resourcing and funding kind of issues because they underpin literally everything that you're doing. | | |
|  |  |
|  |  | P15 |  | I think I'm probably more worried about the more general context of.  How everybody works together in in a bigger sense, political direction in major incidents.  Which can be erratic at best.  And and their engagement in emergency response in advance of the incident. | | |
|  |  | P17 |  | Yeah. Well, it's, it's us. It's us generating the technology and it's us trying to sort of excel it to a way. But likewise, it's us who doesn't have the awareness or or or the training or even the capacity to to kind of really learn different domains, I mean.  Some some of us are fortunate to kind of be quite widespread in our skill sets and and.  Whilst you know.  There's a there's an infant limitation in that in that risk in that degree, some people are a lot less.  So yeah, there's there's an issue there. So it's kind of like how do you address that, you know, yes, you can add in solutions to all in, but you're still adding in. You've still got elements of human interaction there that that's causing a problem. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 223 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Risk Managment Improved** |  | | | | | |
|
|  |  | P14 |  | This is a big issue because I'm not just talking about some sort of central agency that does that.  It's about risk.  So the current work I'm doing on cybersecurity behaviours, one of the insights that's coming through is that inside companies, the risk culture is.  Risk averse or?  Over over protecting and spending too much money just to sort of create crazy defences.  Or apathetic because risks aren't recognised and sufficiently understood.  And so you want to be creating just as you know.  In any company now there are going to be people who have any larger company HR skills and legal skills and probably some health and safety expertise. You want to be having cybersecurity and you want to be having risk management, some really baked into that. | | |
|  |  |
|  |  |
|  |  | P14 |  | one of the key messages from that conference was, but the most important thing UKPLC could do would be to really get its risk of management sorted because, you know, people get fixated on, say, a particular threat.  Without necessarily thinking about what are the harms that that threat is causing and what should we worry about? How much should we worry about so very simple example, judges come from subsequent conversations with National Crime Agency you can imagine.  I'm not saying this is true or not because I don't know if it's true or not, but you can imagine voices inside the National Crime Agency arguing for resource to be deployed to deal with a particular challenge.  And some will be calling for work on illegal migration and some will be calling for work on child sexual exploitation.  Now stand back and just think about the harms. It's very clear the harm from CSE child sexual exploitation is profound not only to individuals, but it affects their education, employability, the knock on effects. It can go through generations so substantial.  Argued. I'm not saying this necessarily, but it could be argued that illegal immigration is quite good in an ageing population if it's bringing large numbers of younger workers in who are eager to work and might end up paying taxes, they could actually be beneficial rather than harmful. So, but you could have two voices, perhaps politically inspired, saying, you know, we've got to do something about the immigration. And of course, we've talked about politics. That might be an important factor to bear in mind in terms of cost. If you create civil disquiet.  And cause all sorts of problems because the the indigenous population is now not happy with all these bloody migrants and blah blah blah. But yeah, so focus there a proper risk management approach which thinks through identifies what the threats are, identifies where the vulnerabilities are, identifies what the, So what questions about what, the consequences, the threat penetrates the target and causes those vulnerabilities.  To to work through. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  | P14 |  | , we need to improve our risk management capabilities so it doesn't rear. I'm banging on about electromagnetic stuff, but then something completely different will hit us and blind side us and it doesn't really matter what the threat is or what the hazard is or what the consequences are.  What really matters is having.  An effective risk management capability.  Skills that are quite widely spread. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 224 of 316 |  |
|  | | | | | | |
|  |  | P14 |  | is the House of Lords. Did a study on this three or four years ago and was identifying that there are serious failings in terms of the capacity and the capability of the country to do good risk management. And that for me is a big issue. | | |
|  |  | P15 |  | if you're looking at risk management, there are the controls that you put in place in terms of preventative controls. So how do you, how do you stop the thing from happening in the 1st place? How do you reduce its likelihood? And then you're also looking at your responsive controls in terms of like the impact that it might have and and how well you deal with it because.  You you might address both of those, and you might still also have some residual risk leftover.  And therefore my my main concern, emergency management's main concern is on the responsive controls, but that's why it's really important and I think this is this probably is relevant.  In terms of like joining risk management up?  Risk management and Emergency Management together. | | |
|  |  |
|  |  | P15 |  | So LR FS Local resilience forums are they are mandated by the CCA and it says that basically or that they're required by statutory guidance that supports the CCA. | | |
|  |  | P15 |  | You can normally each LRF would have their own bit and they can invite people in who can see their documents and they can share shared plans. But they also might say this is our single agency plan but you can see you can see a copy of it. So it means it. It reduces the amount of trying to share encrypted emails and things like that for Security Commission. | | |
|  |  | P15 |  | They basically are a multi agency partnership of people in a geographic area, typically under a police force zone bounded by police force boundaries.  And then they would work together to identify risks that would be relevant to their local area. They would plan and train and exercise together for how to respond to those risks and would work together on things. So that's the sort of they have both. Both are sort of meeting schedule and then also various groups and subgroups which before 2004, they didn't really that that did not exist formally in any sense. It might have done it informally, depending on where you were, but it wasn't required. So it's the way in which.  Category 1 responders in particular can demonstrate that they are discharging their duties under the ACT, and there are also various national resilience standards. They're supporting. LR FS are things like Resilience Direct, which is a slightly clunky.  Information sharing tool. It's basically a big document store. Formative a better word. It's it's nothing fancy, | | |
|  |  |
|  |  |
|  |  | P15 |  | And you then look at, OK, these are the risks, this is how it's impacting this is what we're doing, the OR these are the options of what we can do about it from a preventative and responsive nature.  That you can make sensible decisions around. Well, OK, We're happy to tolerate not doing much about it because we want to rely on our responsive controls. But we know that there is an inherent thing, and if that does go wrong, then we're liable to this. | | |
|  |  |
|  |  | P20 |  | is it's people, it's training.  And creating the the skills in our economy and in our society that have the capability to deal with this stuff. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 225 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | It will mean a higher cost at the beginning.  But it will decrease the cost at the end for testing and verification and all that we are doing today and we'll also have more resilient systems and this is not yet there in any kind of, I would say public organisation or large critical infrastructure operators and that's the challenge that they have. | | |
|  |  | P6 |  | We have to find new ways of building systems and testing systems. So a keyword will be by design. So we should we should securely by design safety and security by design. So we should think about architectures having tools supporting us how we are designing system.  Where our data so the architecture is understood, the system can help me and say OK can help me by the risk management if you do it that way. At the end security it's all about risk management. | | |
|  |  |
|  | | | | | | |
| **Risks and Implications** |  | | | | | |
|
|  |  | P10 |  | There's sometime in the future and I I don't know, this is just 'cause. It's on my mind from conversations we've been have been having and and sort of the work I'm doing. But there's there's again this is sort of database, there's evidence just that people.  Kind of trust in their organisational.  Sort of protections. You know, they might not trust at home, but on the work. I think if they work for government or work in, you know, a a critical.  Part of of of the Society or the financial sector or health or whatever, and so if they get a dodgy e-mail, they'll fall. They won't open at home and they won't open up on their phone because it looks, you know, they've used their intelligence. So they'll forward it to work and they'll open it at work because they believe, you know, that everything will protect them there and that that there's there's, you know, we know that people do this. And if that is kind of terrifying and that's the sort of someone who who thinks they're, you know, doing the right thing and and sort of almost trusting in the systems that we've said are in place.  And and therefore, you know sort of that that sort of cascading effect. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 226 of 316 |  |
|  | | | | | | |
|  |  | P10 |  | So we have the national, you know, cyber strategy. We have the government cybersecurity strategy, every country is coming out with its own strategy at the moment. Good, good on them. Some of them are also coming up with some very narrowly focusing on cyber here. Some of them will say very sensibly coming up with their own action plans. We don't yet have one in this country.  MAD are coming up with their own strategy and action plan. The National Health Service is coming up with its own strategy. You see where this goes. So the fragmentation across the piece, I mean, just as I'm critical of monoculture for obvious reasons, I'm also critical of, you know, abject fragmentation and siloisation because we really do need a joined up approach here. And so that that's that's, you know and and some very strong leadership and not getting quite so distracted by shiny things like AI.  But you know, actually thinking about this and I I sort of mentioned that that kind of shift in gear from.  You know, to, to, to you know, to to a dangerous time. I mean, I think it's we've always been living in dangerous time. Right. But I think you know that it's not as safe. It's not. The world is not a safe place for the geopolitics. Engaging, engaging here. Not not.  Not just focusing on the geopolitics, but, but you know they they obviously kind of setting setting the scene here. But I think you know some some real direction, some some.  You know, there is so many different agencies in in the UK in particular leading on this and then globally it becomes even more, you know, even messier.  So it's very easy for you know, the tech Bros to to do the thing that they want and we have we spend very little money comparatively on on this. So that those those I think are are are key considerations here. | | |
|  |  |
|  |  |
|  |  |
|  |  | P10 |  | We the the the risk of monoculture in security subsecurity in particular is if everyone, let's say, everything government is run on Microsoft because they're very good and you know, I've no criticism of Microsoft. But if it's a monoculture, you get one floor. Great, you've got one floor and it gets, you know, it kind of goes across the piece and there's again just looking at good data. Microsoft, if you if I am a malicious person and I want to you know create a but I'm I'm going to target Microsoft because it is.  It it is buggy and it's going to have, I'm going to get my greatest bang for my buck. I'm not going to be trying to work on something. What is it that submarines run on? You know something that's really archaic, you know? That that's that's less. That's less of a challenge. So those sorts of things. I think that that monoculture in in, in technology and cybersecurity is is a real issue. | | |
|  |  |
|  |  | P10 |  | This goes back to my earlier concern around environmental issues and also speaks to your your your questions around CNI.  Just, you know, keeping the lights on. I was, you know, sort of growing up in the countryside where power cuts were like, you know, whenever the winds blow, we seem to get a power cut. I think this might be casting. This is my back story casting this, this, this, this foreshadowing. But, you know, just just, just, just, just just cut just losses to, you know that that, that, that, that sort of specific we take for granted is is is as a much a problem here. I think you know that of telecoms.  I know that's part of the the critical infrastructure, but thinking about just loss of those kind of basic services kind of water for cooling service, you know loss of loss of of power and we are moving into what you know people are describing is we're moving out of that post war history phase into a pre war phase of history which is terrifying. But you know that that's that's that's an obvious kind of you know sort of attack.  Sort of. You know, point it's a point of vulnerability.  Hacking systems. You just kind of take out those those because it becomes so, so, so essential that was very garbled. I'm sorry. | | |
|  |  |
|  |  |
|  |  | P10 |  | So you see this as a as as the best thing to be some sort of global. So some sort of UK wide.  Strategy and actual plan from it to to address the resilience issue as much as anything. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 227 of 316 |  |
|  | | | | | | |
|  |  | P10 |  | Exactly. But I think it probably it should be, yeah, that sort of thing, you know, so I I just just something that's kind of Co ORDINATED doesn't have to be you know I'm I'm not I'm not you know I'm not I'm not overly invested or you know in my in my trust in in in the ability of the government to deliver on important things here shall we say you're my cynicism was clear when we started but I I think something like that would you know making it whole of society approach that's that's globally would like to kind of push on say bringing in industry you know people are throwing far more money on it in in business initiative than they are able to in government so.  What? What are they learning? What can they share?  Academia again, you know some some great minds and some great work, you know, get those people around the table rather than that, the fragmentation that we see at the moment, with everyone doing lots of, you know, a lot of busy work, how could we join this up and be more than some of our parts? I know that's a terrible cliche, but I kind of think this matters. | | |
|  |  |
|  |  |
|  |  | P10 |  | But | | |
|  |  | P10 |  | OK, I I I have a slightly different. So I mean I think working with colleagues at NCSC, they they are very you know, while I work with the sociotechnical and risk team predominantly, they're very good at. So you don't. So the, the, the, the sort of the very the Uber techies which to just assign unfairly different tribes, it's fairly to these tribes. But for them, you know, the humans, the kind of the wet wear, we are the humans are the weakest link and then the sociotechnical risk group. Of course humans are also the strongest league.  I don't have the data to back this up, so I hate throwing this into the mix, but I think I still want to.  More sort of breaches are, you know, are caught by human spotting reporting, you know, than any sort of automated system. And there's really good, you know, a good story there that people are very good at stopping and spotting things. You hear stories that people realising, yes. Yes. They've clicked on the malicious link, but they're also the one who, you know, who it's a it's a it's a it's it's not like you know, they'll just rip the you know they'll rip it out of the system.  And they'll lose. You know, various proprietary stuff. But so it's like people are doing very clever good things in in lots of places. But I think we, we we are a bit more a bit more up to the idea that you know just clicking on those links is is clearly you know that sort of social engineering attacks are are really critical. And I think we've seen the rise in the number of you know is it something that was on the radio yesterday about the number the rise in fraud in fraud.  You know, so basically online fraud as is now the most sort of common motive you know of of sort of criminal.  Injury that that your average citizen encounters, which is clearly digitally enabled. And so I think the seeing that over into crossover into cybersecurity where where people are vulnerable if not that we think certainly vulnerable, yeah. | | |
|  |  |
|  |  |
|  |  |
|  |  | P11 |  | Now that, sorry, that was my point about I just closing, closing it around. That's the point about determinism. You, you lack the observability to be deterministic beyond not only in detail down, but in time. | | |
|  |  | P11 |  | Right. So so this is something you can you can have all the digital twins in the world etcetera, etcetera. First of all, they cannot reflect exactly what's happening. And secondly, there's a measure of indeterminism about what's going to happen anyway, is that. Is that what you're after? Yeah. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 228 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | Environments like Smrs will only be economically viable if they use technology that isn't currently regarded as being appropriate to those kinds of.  Safety critical environments, so you can't always get the sensors you want and the places you want. You can't always have individual wires going to every last sensor because there isn't the space and they're sealed for life.  So you end up having to do in make inferences to parameters rather than.  Bring them directly. May not be able to measure a particular pressure in a particular place. You may have to make some form of inference.  Using and here it comes using a digital twin.  And and so I see quite a lot now that's that's a sort of development beyond what I referred to earlier, which is that prognostication prognostics and diagnostics there we are.  The prognostics and diagnostics are effectively done, even if they may not be advertised as such against a digital twin.  And I think the question is. | | |
|  |  |
|  |  |
|  |  | P11 |  | So one of the areas that really did did concern me for a long time, and I think people are now doing something about it is the stability of the grid.  It's it's essentially it's a, it's a non linear mathematics. It's a mathematically a nonlinear control system challenge to have small amounts of generation interspersed with small amounts of of consumption.  In a grid that was designed to be a central generator against largely resistive inductive load, it isn't anymore.  And I don't think we.  I can't. I just. I don't. I don't know whether we woke up to that fast enough. | | |
|  |  |
|  |  | P11 |  | I | | |
|  |  | P11 |  | How do we know that this is going to wait?  How do we know that that digital twin is integrity is intact? | | |
|  |  | P11 |  | Right | | |
|  |  | P11 |  | My concern, and by the way I I don't quite know how much of your interest is in the adversarial actions against the CNI and how much is just about wizzy technology for building the CNI. But I'm I'm more more concerned with the the adversarial action because that's where I come from. That is my, my history, my background.  I see security is being taught too much as an additive activity.  An existing system design.  Particularly one that has been through all the safety processes and has been deemed to be, you know, just just fantastic, that's just excellent. So now with your security nodes, please do whatever it is you do, but don't touch our system because it's, you know, because it's fine now we want to put it online. So we you'll probably want to put some do some stuff around it. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 229 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | I don't know, but I would like to ask the people are writing them 'cause. I think it's their. I think it's their duty to be able to put a confident back confidence bound on what they're producing.  But at least that's a terribly old fashioned engineering principle that every measurement comes with a confidence interval.  But I don't see that happening and I think in the case of artificial intelligence.  Even less so than I mean true artificial intelligence, even less so than machine learning. And I think a lot of what we're we're talking about really at the moment is machine learning. I think artificial intelligence is a word that's as an expression just picked up by the marketing people. | | |
|  |  |
|  |  | P11 |  | No client nobody knows what to do about it. Nobody really knows how to put a watermark into something to say this really hasn't been.  Tampered with because?  Ultimately, it's not the technology that you're trusting, it's the person who's operating the machine. | | |
|  |  | P11 |  | but I can't work out why I only mention it simply to say that not everybody agrees with me, but I believe that there is a relationship between the level of observability and the degree of determinism and.  In the system.  And you can't.  Ever achieve perfect observability?  Because there aren't enough days available to us or there aren't enough census or whatever. So to some degree you lack a. Your determinism reaches a kind of threshold and I use the example of something like a laptop or a or a Windows Server. | | |
|  |  |
|  |  | P11 |  | Let me pick through the assembler and see if I can work out what it's doing.  It's just unbelievable and it introduces the kind of complexity which is anathema to the kinds of things that I'm looking for.  Yes, correct. | | |
|  |  | P11 |  | Yes | | |
|  |  | P11 |  | It | | |
|  |  | P11 |  | Yes | | |
|  |  | P11 |  | but just in terms of let's call it artificial intelligence, let's even just call it machine learning, one of the rhetorical questions I think that.  And and bring it back to that digital twin for the for the weather forecast.  How do I determine the limits of my confidence in the outputs of the machine learning algorithm? | | |
|  |  | P11 |  | He yes, I think you will never get perfect observations. You have an engineering or science background. There is always. There's always a probability density function around anything. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 230 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | Yeah, but they're as useful as the weather forecast. I find it immensely useful that, and they're getting better because because the cell size is getting smaller and the observations are getting more numerous and more frequent. | | |
|  |  | P11 |  | Oh well, since you are from the software background, I would share with you a completely different concern. I'll change tack completely. I think it's the way that we write software is a concern to me. It's.  I saw an article in the IEEE which I haven't read, but really resonated it said. Is this the year that we did finally deal with bloatware?  What it's talking about, I think, is the tendency to. | | |
|  |  | P11 |  | Let's | | |
|  |  | P11 |  | And | | |
|  |  | P11 |  | Well, I just around it and I just reject that model utterly. Now I think as we put the CNI of the future together or even deal with the legacy C and I, we already have, we're going to.  Have to adopt some of the more sort of system theoretic type stuff that Nancy Leveson talks about.  Except in a way that's practical. Sorry, Nancy. In a way that doesn't require more hours than there are in the universe to model the system.  And for the safety people.  Stop focusing on random.  Unrelated, uncoordinated.  Mechanical like, you know, like Poisson function type, you know. Oh, oh, here comes another one failures which we can model from historical behaviour. Where's all the system? Is it systemic? Systematic anyways.  Where are the systemic risks? | | |
|  |  |
|  |  |
|  |  | P12 |  | That's what I'm thinking as well. Yeah, I'm trying this as well, but try to get GBT to actually generate code. It's it's pretty hit or miss for anything but like kind of, you know, yeah. Basic unit tests. It's not so great. But in years. Yeah, sure, maybe. | | |
|  |  | P12 |  | Yeah. Yeah. And and like, more and more like code generated code, you know like LLM generated Python then yeah, I don't know. You know that that can be that could be confusing and difficult. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 231 of 316 |  |
|  | | | | | | |
|  |  | P12 |  | And computing, oh, God no, I don't know if this is the answer you're looking for, so I'm happy to revise it if it isn't. But the thing that is has been on my radar and this is very much kind of a parochial thing for me, is that I think that the kind of the end of the Pax Americana and a return to more ad hoc and sustainable conflict is really the biggest change that I'm tracking. I think that we've been playing security on easy mode because.  Disrupting critical infrastructure.  Would have been out of bounds up until very, very recently and for a variety of reasons and sort of, I would say beta tested by ransomware crews who do this for profit and operate with impunity, you know, within Russia typically or North Korea, you know, we've seen that actually there won't be probably a military response even to critical infrastructure.  You know, attacks, at least so far, and I think that that.  New reality is created. What I believe to be the most dangerous kind of change recently. Yeah, it's not a check answer, but it is. It is my actual answer.  Oh good. I'm still out of here. | | |
|  |  |
|  |  |
|  |  | P12 |  | when I look at AII really see this is almost like the way I would look at like a compiler where like we had assembly, right. And then there's this compiler that's interposed between you and the actual assembly code.  And as you work your way up that stock, you know with Python I don't even know what's happening at the C++ binary layer, let alone what's happening assembly. And now I think like AI and generative AI in particular has really interposed at a level above where, you know, I know people who are using, you know, llms to generate Python. And that's just another layer of interposition. And I think that as AI interposes more and more in that stack, the more it becomes difficult to discern what's actually happening. And I think to this question, yeah, that does potentially make it harder to discern whether something was.  Misconfiguration or yeah, an an attack. | | |
|  |  |
|  |  | P13 |  | And there's always potential for the misdiagnosis mistreatment, which falls into the whole range of patient safety or lack of provision of treatment.  I think that there's that, but.  I don't know. Possibly. Possibly if the the whole system becomes corrupted then potentially, but I think it's less likely that an individual patient level. | | |
|  |  | P13 |  | Yeah, the lower the lowest be the reactive, I mean that that's inevitable.  But I think increasingly.  Economic pressures will probably be the thing that drives it more than anything else.  But you know it, it does require quite a change that requires it requires individuals as well.  To really take more responsibility for managing their own health as well.  Yeah, and it helps them to do so exactly. | | |
|  |  |
|  |  | P13 |  | So the major incidents would be somebody messing up the model, particularly if it was in subtle ways. | | |
|  |  | P13 |  | You know anyone who voted for this party would would get you know.  Subtly less less treatment than those who voted for voted for that party.  Golly, that they, yes, yes. | | |
|  |  | P13 |  | Desperately scary. So. So there's all sorts of, I mean, they're not, they're not really the sort of critical infrastructure problem. They're more just a a horrible threat. Yes. Yes. Yeah.  What's getting back to the sort of emergent crisis?  What sort of combination of incidents and errors could really mess things up in the health sector, do you think? | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 232 of 316 |  |
|  | | | | | | |
|  |  | P14 |  | Passed | | |
|  |  | P14 |  | the Internet of Things is another major game changer, because when the whole world is connected up.  And when you could actually, you know, a sort of some some spotty youth in a basement in Melbourne just wanting to have fun, not necessarily trying to destroy an enemy, but just wanting to, you know, have a little bit of a laugh.  Can connect through and get into some Internet of Things link which then breaks into a bit of the critical national infrastructure. You've got huge challenges there, so when you get the democratisation of technology and capabilities that quantum might offer, it won't initially, of course, but might eventually offer.  Certainly with Ji and ML does offer combined with an Internet of Things which allows everything to be joined up in a. | | |
|  |  |
|  |  | P15 |  | Yes. Yeah. And anything I would suggest, anything where you've got a huge amount of infrastructure which needs to have surveillance on it. And I don't know around nuclear sites, if you don't have exonomy, you've only got X number of cameras and X number of.  CNC the civil nuclear Constabulary. They can only be in certain places at certain times. Therefore, like how well see you. Are you managing the the security?  You know, security awareness.  And situational awareness around risks that are physically present at the time and also virtually present and things like that. So.  I think again there are opportunities, but again there are opportunities and threats for those systems to be infiltrated. | | |
|  |  |
|  |  | P15 |  | Yes, so this is this is fascinating. 'cause, you're you're saying it's nothing to do with whether AI is good, bad, predictable, unpredictable. Whatever. The sheer fact that it is a change in the way people are going to do things is itself does bring its own risks.  Yes, that's very interesting. I I think I don't think that's, I don't think many people have made that point that's that's really that is really interesting. Yes, yes. | | |
|  |  | P15 |  | Yes, and I the same. The same goes around things around severe space weather.  And the impacts of solar flares on on things and how you start to look at risks and how they would manifest themselves.  So how that could manifest itself, particularly within a particular infrastructure in in terms of like the rail industry of understanding cable, a lot of those risks would look similar.  To a national power outage or a regional power outage, which there's been an awful lot of thinking and mostly the thinking is that would be fairly, fairly catastrophic, but it would be so catastrophic that literally everything else would have failed at the same time. So trains wouldn't be your last issue. And there's a there's.  I think the the biggest risks are the ones where.  Things are so uncertain about where they might happen or how it would trickle out, or we didn't. We haven't done the thinking around those things, and I think the AI and those opportunities are.  They are inherently unknown because we don't know what we're going to do with them and if you don't know what you're going to do with them, you can't know what that then would mean. Actually, if you did implement that in a very benign way, that itself might introduce additional risks and and hazards that we can't anticipate yet.  And we also can't necessarily anticipate even the people who are intentionally planning and designing how they want them to work or want them to do things, how people then interact with them and would engage with them and start using them when they're out there doing their own thing and aren't sort of being heavily controlled. | | |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 233 of 316 |  |
|  | | | | | | |
|  |  | P15 |  | So you can't control how people necessarily use devices. | | |
|  |  | P15 |  | Definitely like if you're.  If you're looking at data to try and understand what's going on in a major incident, I mean back in the day, people would look at Twitter and see what people were saying. If if sort of hypothetically like that that exists in that context. But half of that stuff is misinformation or is about something else or you're using some kind of tool to not like APC going in and looking and saying, oh, I've just seen this, this person's reported this or that person's reported that or.  I know they're analysing the 300 calls that will come into it to make a control room, to understand, OK, what are the key bits of data that we can get from that if those things are being fed by misinformation and disinformation, then that could lead you to.  Deploying the wrong kind of resources in the wrong quantity to the wrong place. They could be at risk.  And therefore you would be delaying. You would either be running the wrong response because you think a different kind of incident is happening. I I you think a firearms incident is happening rather than a bomb.  With with screws and bullets in it that made people look like they had firearms injuries.  It is a firearms instant because my friend's just been shot. They haven't been shot. It was because of the.  Shrapnel and stuff in the in the bomb. | | |
|  |  |
|  |  |
|  |  | P15 |  | And therefore there are opportunities for things like that absolutely to be either intentionally or unintentionally.  Suede by AI doing that thinking for us.  So you you could potentially think a place is safe and choose that for where you want to put your all of your resources. And it turns out I know it's underwater or or it's in a in an in an area which could easily be that threat from whatever the risk is. | | |
|  |  | P15 |  | AI and computer technology like is the risk that is is worrying in terms of or it's it's an unknown and it's the interconnectivity of the sort of asset management systems and data management systems and all of these things are sewing interconnected that if you have a failure in one and sort of not being able to understand in advance what the ripple effect would be on those systems.  And I think that the more things are automated, the more things rely on on additional technical systems and technical solutions.  Then it's sort of increasingly interwoven with each other and then becomes increasingly difficult to understand.  Where that happens. | | |
|  |  |
|  |  | P16 |  | Probably try to design new systems that are not fully automated but work hand in hand with humans to kind of monitor and respond to cyber attacks in a way that's really effective for organisations.  So that's the I think probably the high level answer and the low level is try to train.  Retrain everyone to with working within those organisations, not cyber security specialists.  The all the employees to help them.  Understand the new AI threats. So those I was just reading before Oracle the the new report by the.  Your National cybersecurity centre.  Where on AI threat and who's going to make the most use of it. And they were explaining that we're going to have to train people to understand that now any e-mail that you receive from anyone can be coming from an AI and not from a human.  Still be very, very persuasive and be be perfectly. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 234 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | Exactly an exact reflection of a of a authentic e-mail. So training people to not trust the first site, everything they see and they get in their inbox and and make decisions accordingly. So I think we're also going to have to in terms of human interactions with machines that we're going to have to redefine our understanding of.  Trustworthiness and.  Protocols for people to make important decisions.  And to validate and authenticate authenticate.  The content of information, so I think it's gonna be an interesting few years to kind of redesign all of that and to retrain a lot of people. But it's gonna be an evolution, not a revolution, I think because now AI becoming so embedded into everything so.  So. So for AII think it's gonna be, you know, massive probably.  Communities for cybersecurity companies trying to offer products and services to the critical infrastructure to adopt those new technologies and and.  For AI and for Quantum, I think that's. | | |
|  |  |
|  |  |
|  |  | P16 |  | Interesting | | |
|  |  | P16 |  | Yeah. So, so because I don't know if you've seen those presentations where the people say like the quantum people say, well, when encryption is gonna be brought universally broken by a quantum.  Computer all the secrets that have been collected over the past decades, they gonna instantly become.  Transparent to anyone and then people will use AI to kind of craft.  An understanding of the present based on past transactions and past.  Communications. So we need to now protect or.  For a future.  For a quantum future, and there are some existing mathematical and ways to do it without quantum technologies. But even if it's discovered in 30 years from now, we have to protect secrets now.  If these secrets need to be maintained for 50 years, for example. | | |
|  |  |
|  |  | P16 |  | Well, first I I I I I I I sleep very well and I tend not to be kind of too disturbed by by that.  But I think that probably the what, what? What concerns me is that.  The the the the label of interconnectivity that we are implementing with all systems being connected to all other systems using underlying technology that bricks that we kind of.  Place here and there without often.  Fully understanding all the interdependency that we are creating.  Might very well.  Create a system where risk is being amplified without us being able to understand how it propagates within the system and leading to you know, a common event that could trigger a general collapse of systems.  So this lack of mission, lack of understanding of the interconnectivity and interdependencies, and and I'm not only Speaking of, you know, explicit interdependencies of systems being connected to each other, but also the open source. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 235 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | Software that we that are used very broadly for you know free that you get from Itab and other places and repositories of.  Bits and pieces of software, then they're they're being used for those major.  Uh. Uh umm.  Control for critical infrastructures and then suddenly we realised that we depend on.  Crappy programming by done by a single person that everyone assumed was very safe but no one bothered to check, and then we end up like the heart bleed or incident or and then my concern would be that instead of discovering it and being able to fix it without anyone having had the opportunity to leverage it for an attack, we we find it about we find out it during an attack and after our systems have collapsed and.  And we end up in situation and you know our societies.  Are not ready to absorb.  Some types of collapses of certain systems. I mean, we've seen it during the pandemic. | | |
|  |  |
|  |  |
|  |  | P16 |  | You just just you mentioned a phrase I hadn't encountered risk propagating. How does? | | |
|  |  | P16 |  | You know the the the, the system replicated and just kind of.  Went a wire and just went all all around the world and paralysed a lot of companies so that that's the idea of propagation. You know you have something in mind that may be a very contained attack. But then because you it's becoming so complicated and so complex. Even for the goodwill attacker, you know it cannot understand all the.  The complexity of the whole ecosystem and might just produce results outcomes that they never kind of actually wanted to to achieve. So that's that's you know this kind of propagation, something that gets out of control.  And not because someone wants to pose major havoc, but just like they didn't think through exactly and they didn't have a clear map of the interconnectedness of our digital ecosystem.  Exactly. Exactly. | | |
|  |  |
|  |  | P16 |  | Yes, yes. Or even have a country and and and the other I think the other. Yeah. So the attacker doing that for I I think for two reasons possibly the one is the complexity of the whole system that no one can can truly understand I think or.  The other one is that those tools are gonna be so powerful, but they're gonna still be used by very sometimes.  Unskilled people. So, and that's you know that. So that's what we see with Aiai benefit in general. And now I'm I'm thinking I'm talking in general AI benefits the most to the to the more unskilled and the more junior people because it enables them to make such a high jump in quality. But if you're an expert already, if you're a very expert hacker or very skilled hacker, I don't think AI is gonna make your life.  So, so much better. But if you're a script kiddie, or someone who starts out in hacking, it's gonna give you super powers that you may have no way of control being able to control. So. So I think that, you know, this kind of out of.  Crisis might come from a very skilled attacker not understanding fully grasping the complexity of the system and then not being able to control their attack, but also from the fact.  But very, very unskilled actors are gonna have access to super powerful tools.  That are gonna be sold to them by those mid level.  Hacking organisations or networks and who knows what they're gonna be using those for? I mean, I study hackers and most of them they're very young, quite immature, very impulsive. | | |
|  |  |
|  |  |
|  |  |
|  |  | P16 |  | To young people when they start out, you know very often, you know, we don't care too much if they scrap them and you know that we we ensure that they're not too fast and they're not too. So. So that it. That's the kind of analogy, you know, giving a Ferrari or a Porsche to someone who's just had their driver's licence. Usually it's not a very good mix. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 236 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | Yes, yes, yes. Because the tool they have at their disposal has some level of, I wouldn't say consciousness, but has some level of autonomy and automation that will actually that makes it.  Do things at a scale that.  An untrained or unskilled mind cannot comprehend.  So they just see, you know, a machine able to.  Achieve certain things, but without fully comprehending that how it it it's doing that and then they're not understanding the all the all the implications of their request in terms of.  Neutralising or harming the whole you know the the the targets systems. | | |
|  |  |
|  |  | P16 |  | Well, it's it. Well, it's it's a it's it's a very I mean it's not. I'm not claiming it's something very complicated. It's just like the fact that when you have those interconnected interdependent systems and you have like a very autonomous tools now being developed to attack or to defend. So you have machines that are making decision just like in the stock market when you have an initial, you know, a tiny event.  Generating a cascade of decisions.  Decisions by, you know, in microseconds by.  Software that is trying to beat the crowd. So I think that's why we're probably going to see when when AI is going to be manning a lot of our cyber defence systems and AI are going to also attack and are going to let loose by malicious actors to attack certain targets. It's very possible that.  You know, they didn't think of all the implications and the the attack might get out of hands and and and keep on propagating outside of the initial bounds of what was planned or envisaged. And we end up with, I think the.  What's the? What's the attack that you know what? There. What's what's happened with the Russian malware?  Can't remember one. I cried, so not pity. I wanna cry 2 pieces of malware that were supposed to be contained to attacking Ukrainian.  Organisations. But because of the the fact that a lot of Western companies had outposts in Ukraine were operating in the Ukraine, then it was used. | | |
|  |  |
|  |  |
|  |  | P16 |  | I give giving a Ferrari as a first car to someone who just like to an 18 year old full of testosterone, who's just had their driver's licence. You know, it's not a good that's there is a reason why we give second hand cars. | | |
|  |  | P16 |  | So yes, so so I was gonna ask for, you know, kind of like a story, a possible series of incidents. So this is it's. It's a little like the sorcerer's apprentice, isn't it? It's the the the UN unskilled hacker, given this insanely powerful ready package system that then that then also goes beyond, they don't know, the unskilled person doesn't know how to limit it, doesn't know how to focus. It doesn't know how to target it.  And therefore, you know, all of a sudden some hospital somewhere.  Is completely wiped out or or yes yes. | | |
|  |  |
|  |  | P19 |  | Am but the complexity of systems is is I think something that needs studied more so in terms of trends as game changes much more complex systems.  Human human incorporating. Yes, yes.  Human yes, sources of of risk. | | |
|  |  | P19 |  | Also, by the way, humans there's sources of problem solving. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 237 of 316 |  |
|  | | | | | | |
|  |  | P19 |  | Probably companies that are are designing systems instructs probably do some of the there's already yes, because they they have forums where they talk to users and they they tried to build the they tried to specify the software so that it will six.  You know what?  The users need what I'm saying is alongside of that, the you you have to think about the risks of things that will go wrong.  Probably you, you you know, you're you're deciding how much redundance you're redundancy to to fit into the technical parts of systems.  You have to think about how you you deal with the the likelihood of people be compromised or people making mistakes. | | |
|  |  |
|  |  | P19 |  | I suppose people shouldn't really be be given more more access rights than than they need umm.  That, that, that could could be seen as as rather draconian but but these things that we have to be taken into account, yeah. | | |
|  |  | P19 |  | I mean, people in, in organizations who perhaps don't have the the the maybe have access rights that they shouldn't.  They they can inadvertently to talk.  Yes, you you can.  It can be subject of of cyber attack and then you know we have and then I'll pay for enough and yes.  So I think that's often the of her faults.  Get injected and so yeah, that's interesting.  So it's not.  It might typically be the big boss or someone who has lots of authority, but well, the this is part of the organizational tree. | | |
|  |  |
|  |  | P20 |  | Yeah | | |
|  |  | P20 |  | So you have those sorts of arguments that are framed in geopolitical terms, and they're about the emergence of, you know.  Sort of arms race dynamics, if you like, around AI software.  In terms of.  Software development for critical infrastructure. I don't know a huge amount about it, but historically it appears to be riddled with vulnerabilities and weaknesses in terms of if you look at the state of secure software in those sectors.  Not a lot of protection around lots of industrial control systems. Wanna cry virus spreading globally affecting the NHS, systems that are still running Windows XP.  Legacy software not being able to update it being used globally, which of course creates a whole new, you know, levels of vulnerability.  Yeah, I mean, I I just think it's a, it's a market which.  Is pretty pretty weak still in terms of security, I I I attempt during the pandemic they had the Aspen Cybersecurity Summit, which is one of these big American events. And Alex Stamos was there, who I'm sure you're you're aware of. And he he said something which stuck in my mind, which was that. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 238 of 316 |  |
|  | | | | | | |
|  |  | P20 |  | . Well, I think, I mean what, one of the things that.  I'm concerned about in terms of software development is.  You know, this idea of sort of rush to release of software, particularly AI platforms, because you want to get ahead of other commercial operators, but also other countries. So you have, you know in my view open AI releasing ChatGPT in a in a way and form that I don't think was entirely responsible where there were numerous vulnerabilities which were observed only after it was released.  And I think you know the this rush to release this idea of, OK, well, we won't. We won't do sort of all that much in the way of proper security testing or risk assessment of the software will just get it out into the into the world and let you know Crowdsource that and and let others figure out what the vulnerabilities are. I don't think that this is a particularly responsible.  Process for software development in the context of AI technologies, and I think it's historically been the same for cyber. We're caught between wanting convenience and wanting ease of use, but but not having very secure products. So I think this has been a feature of the political economy. If you like, of of cybersecurity.  So I think that there's some concerns about software development and how the the the regulation is put in place around.  Commercial competition over new products, which might create risks, including for national infrastructure and then layer on top of the commercial competition. You've got the geopolitical competition where producers of software are saying.  Don't regulate us because if you do, China will beat us to general AI. | | |
|  |  |
|  |  |
|  |  |
|  |  | P22 |  | It really depends on the regulators, doesn't it? Yes, most of our infrastructure is.  Under regulation rather than anything else, and the regulators over the past 20 years have been focused on reducing consumer costs.  Rather than service resilience, so unless the regulators change their stance, I can't see, you know, I mean, I'm in the Thames Water area. Yeah. I can't see Thames Water changing its policy unless it is quite heavily pushed to do so.  Because you know so much of the industry, the that supplies this infrastructure is not owned in the UK and so it's only really at the point of use that you can regulate.  And that has to be by regulation in terms of.  Measuring, you know, the impact of brakes, so going back to the Nat structure, you know it's it's crude, but it's a structure, it's it's availability and we're you know and it introduces this concept of user hours and a concept of lost user hours is a really useful change in focus for the IT guys.  So we spend a lot of time, you know, changing people's vocabulary in the BCS, who think that software resilience is the same as service resilience. Service resilience is about lost user hours, software resilience in terms of the ability of a software component to recover. Both are important. If you start with the lost user hours, you can then start homing in on where to improve the software resilience of component. | | |
|  |  |
|  |  |
|  |  | P22 |  | And you know, if there's a rising distrust of this stuff.  You know? Yeah. God, it never works. Oh, God, it never works.  Which is terrible because you know, like, you know, I came through the IT industry when it was a glorious future and we all thought this was good for humanity, good for society, good for people.  It's turning into a threat. That's a worry. That's a worry. But anyway, that's not really part of critical national infrastructure, is it? So back to critical national infrastructure. How do we see the technology changing? And I think my view would be that given.  Most infrastructure industries have legacy software that's 40 years old. They're probably slightly guess it's 50 or 60 years old. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 239 of 316 |  |
|  | | | | | | |
|  |  | P22 |  | Yes, because we're getting more and more and more dependent on electricity and telecoms.  Those two, I mean, that's just it, isn't it?  You know, I I mean I I go walking with a group of retired pensioners and it's amazing how many times the conversation as we walk along turns to software failures and difficulties with the Internet and difficulties with, you know, IT systems that aren't working, you know, so it's, you know, there is nobody who isn't actually impacted by if this stuff goes down or it's difficult to use or it breaks.  Society, but you know it's most people now use their phone to do something which uses the Internet at least once a day.  Now, sometimes you can say you know is there a cost to the economy if you know Pat doesn't get in touch with me about supper? No. But yeah, it's it impacts the sort of quality of life. | | |
|  |  |
|  |  | P22 |  | But you know we have. So we have this big disconnect between people. You're familiar with it and understand the problems and people who are not familiar with it and don't have the vocabulary to understand it. And it's probably a vocabulary around systems thinking rather than it specifically, but certainly.  If, well, again, thI was saying that which spent several hours in discussion with policy advisers in gsit, and they were really nice guys. You know, one of them had an MA in measure Portuguese mediat, I think, and seamlessly gsit policy advisor on supply chain software supply chain. And actually she turned out to be quite bright because she came to a workshop and she had actually got it. But.  I shouldn't be having to be teaching people about.  You know the others are. None of them had any sort of STEM education, OK. And so systems thinking is a bit difficult if you don't have any of that. And so this was saying, well, she happened to be having a meeting of her research groups. And between them they listed like 130 people across the various government departments they work with. Now, remember, she is focused on infrastructure. So this was transport, this was.  Probably Ofcom. I don't know. So the 130 people and none of the people that they were in contact with had shown background.  Now this is quite frightening because I think it's quite a big change. I mean, certainly people I knew with science backgrounds went into the civil service.  Maybe they've all mustered out. | | |
|  |  |
|  |  |
|  |  |
|  |  | P22 |  | So who's going to look at an it guys aren't good at reading contract?  Why should I be yourself? So it's a big job. And so some of the procurement people we talked to on the working groups were really concerned about this. But you know, again they were trying to find somebody who was aware enough of the problem to start talking about it. | | |
|  |  | P22 |  | But no, I mean I it was slightly different train of thought it was. How is it going to change?  And I was thinking actually it may not. | | |
|  |  | P22 |  | You're dependent on boarding component. You get, you get no support from procurement, you get landed with impossible contracts, like if it breaks, it's your fault, not the suppliers fault. | | |
|  |  | P22 |  | Procurement doesn't have the capability of looking at software contracts. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 240 of 316 |  |
|  | | | | | | |
|  |  | P23 |  | Lot it's it's become a major concern.  I I also work for a law firm.  We represent only startups.  Or formal advice at the moment is not to accept investment at all from China.  It's too risky and it can essentially get you into trouble with federal regulators.  And there's nothing you can do if that the Cepheus process of its triggered.  There's nothing you can do it.  The issues pertaining to any data, not just things, but also any data that is sensitive, which is soon soon people are gonna figure out that all data are sensitive. | | |
|  |  |
|  |  | P23 |  | And so right now it's things like location.  Umm, but you know in the US we stopped the acquisition of Grinder which was a a kind of a a dating app if you will for people who just wanted to have sex.  And what the kind of behind the scenes there is that a huge number of servicemen, we're using it and the the.  So the US government stepped in and blocked the deal.  And so I don't think if if you were designing such an app, you would ever think that the government would show up and block right?  Umm, so the supply chain issues, I mean as you know here in the UK, the amount of pressure we put on your government to remove Huawei from your stack, we're doing that internationally and we're trading on that, the nations that umm are willing to remove while Wei and other Chinese from infrastructure from their telecommunications get other benefits or intelligence sharing and other types of favors.  I'm so it is a major preoccupation in the US right now.  Linked to Taiwan and you know, whatever happens and whether we can get a silicon factory going. | | |
|  |  |
|  |  |
|  |  | P3 |  | Because of the danger of interference or. | | |
|  |  | P3 |  | And and it's sort of nature of the threat that sort of kind of while you know there's there are additional kind of risks that from cyber point of view that wireless introduces that.  But there's this sort of kind of space.  So one of the sort of issues with this smars and microreactors in particular is that you don't have an awful lot of space for for equipment.  So that sort of pushes sort of people to think about kind of wireless sensor networks and stuff like that because you don't have kind of maybe as a support, I mean again, so this is all ideas that at some point need to hit regulatory reality. | | |
|  |  |
|  |  | P3 |  | so the so the implications is that we have all of these kinds of potentially advanced digital technologies, advanced instrumentation and control as they call it in nuclear kind of operating in these facilities.  And then the sort of question is, is like what are the risks that introduces right?  And I think we're still a relatively early stage of understanding what those risks are which is good for people like me and you because we want to do research right. | | |
|  |  | P3 |  | You know, wireless is a technology that kind of is rarely used, let's say in or used with a lot of caution.  In in this space, because you know because of the. | | |
|  |  | P3 |  | It doesn't really matter too much, but if if a if a sort of system that's doing 70 semi autonomous control based on sort of some machine learning model, well I kind of want to be able to scrutinise why it's giving me some sort of, you know suggested, you know, behavior that I should follow, which is sort of important I guess. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 241 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | Privacy, presumably, is not a big deal. | | |
|  |  | P3 |  | Perhaps then, of course, this nuclear security right?  So theft of the material right is it is a huge topic. | | |
|  |  | P3 |  | Sort of set some, you know, set points or actions and stuff like me configures.  There just to process.  So there's a whole class of attacks about sort of, uh, manipulating the input to the to the controller such that it has a an incorrect kind of perception.  If you like of what the real state of the system is which causes it to behave incorrect, give you correct. | | |
|  |  | P3 |  | And some of that is still about I I think understanding the nature of the threat right in practice.  You know, there's there's a lot of academic work about, you know, attacks to machine learning and all this kind of stuff.  Some of it, you know, I've done a little bit in that space and.  But some of it still feels very academically and then.  Yeah, exactly.  So what's the real risk in practice, right. | | |
|  |  |
|  |  | P3 |  | Uh, how do you operate your facilities? | | |
|  |  | P3 |  | Or or scrutinize at least the decisions that they've made. | | |
|  |  | P3 |  | Uh, and and and sort of try to engineer a systems in a way that this sort of resilient to all of these things as possible and some of that is about kind of making them, you know, Harding them in the 1st place.  But then, like I say, this sort of thing, can we detect you know, when things are going wrong? | | |
|  |  | P3 |  | You know, there's this probably talk about it a bit more when I talk about nuclear, but there's this sort of.  You know, course the applications are things like machine learning.  To I don't know for optimization predictive maintenance, you know, those kinds of technologies.  And of course uses of machine learning for cybersecurity, right? | | |
|  |  | P3 |  | We can use it to do detection, which introduces risks and that you know, risk of exploitation and and, you know, issues around explain ability of machine learning.  Like how do I?  How do I make sort of decisions based on what these algorithms spitting out at me and understand what's going on? Yeah. | | |
|  |  | P3 |  | Difficult to I'm make them accountable, as it were, for that decisions. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 242 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | And for that, I think we kind of need a little bit more research like you know systems he research where we build stuff and kind of say, OK, this is, yeah, they said, yeah.  Test case exactly.  You know, this is this is the sort of, yeah, this is actually what the risk might look like.  And and these are the sorts of tools or procedures, methods, whatever that you should put in place, be that sort of from a hardening of the technology point of view or thinking about the technology and the context of an architecture or a system.  There's a whole right. | | |
|  |  |
|  |  | P3 |  | It's, you know, if you think look at Sellafield again, some of it's around organizational culture. | | |
|  |  | P3 |  | That's how you kind of get regulatory compliance.  So I come to you with an argument case and provide it to you.  I you know, for stuff like machine learning, AI, autonomous operations, digital twins, you know, the the regulator at the moment doesn't really have the tools and methods to sort of determine whether you know actually what you're in, the evidence that you're providing is correct, right? | | |
|  |  | P3 |  | So there's there's, like, stealthy versions of that that are very difficult to detect and stuff like that.  And AI you for sure, could imagine being applied to generating those sorts of attacks. | | |
|  |  | P3 |  | So all of the so the one question is, is all of these kind of like poisoning attacks adversarial examples and all this sort of stuff that could affect machine learning models?  Could they be sort of used against these sort of machine learning enhanced control systems?  Close them to do something silly right?  So that that's sort of maybe another another area, but yeah, you all sorts of kind of maybe interesting and horrible things. | | |
|  |  |
|  |  | P3 |  | So I mean, yeah, I OK my, my my opinion is it was sort of rather not very complicated but but basically there was a suggestion that foreign nations had to sleep a malware what they were calling sleeper malware sort of starting systems at Southfield.  Well, that's not good. | | |
|  |  | P3 |  | I could, I think if you know outside of just doing the, you know doing the the the trip or whatever it is that just to disconnect to contain the issue.  We sort of really need to understand what's happened really quickly. | | |
|  |  | P3 |  | Do you have the contract language in place where they're obliged to support you if something goes sideways, all those sorts of kinds of issues, so they kind of become essential to your business continuity.  And so I think people are just starting to wake up to this now as a sort of a bit of, you know, as a sort of significant issue.  And we're still very early. | | |
|  |  | P3 |  | Uh, that's being shipped, right? | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 243 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | So if if yeah, if privacy sort of kind of takes any form in this space, it's around the sensitivity of the information right from a from a adversarial point of view.  So there's this kind of in nuclear this idea of S NI sensitive nuclear information and which basically is, you know, stuff that you don't want bad people getting called off.  You know the nature of the material that you've got.  How much of it is?  Where is it? | | |
|  |  |
|  |  | P3 |  | But but but I think what the risk is is that there's people, the risk is, is that what what happens is the people like close, we just get a bit too focused on the technology, right?  I mean, this will probably she's not singing to the choir.  But you know, we just get a little bit too focused on the technology and think of and sort of fail to understand how all of its applied in a social technical system, right. | | |
|  |  | P3 |  | So that's the kind of smart grid stuff, and I suppose you know, in with all of that, there's this sort of use of cloud services, of course.  Which changes sort of the nature of.  You know where is the organisational perimeter?  You know, where do you risk?  Sly and all this kind of stuff, that that sort of is different to the way it was before.  And then uh, I think see an awful lot of it. | | |
|  |  |
|  |  | P3 |  | the thing that we're most concerned about is nuclear safety, right?  So any so any kind of cyber, cyber induced you know?  Nuclear safety related incidents or release of material. | | |
|  |  | P3 |  | I mean smart grids is a different topic where of course privacy was a huge is was a huge issue | | |
|  |  | P3 |  | Most of the scenarios that I've kind of thought of that we thought about in the nuclear space, the kind of, yeah, it's some controlled or uncontrolled trip over the reactor, right? | | |
|  |  | P3 |  | And if you have the likes of SMR, which would so so the kind of general conversation with SRS is, that's possible.  Remote small nuclear safety.  Sort of sort of.  Equation has changed.  Then there's sort of risk shifts little bit to be more about nuclear safety like you have this thing in the middle of nowhere with not many staff an increase risk of somebody sort of stealing material. | | |
|  |  |
|  |  | P3 |  | And if you're using digital systems to support remote surveillance, physical protection systems, or this kind of stuff as part of a blended attack, then theft of material is becomes a bit of an issue.  And then the other kind of sort of potential shift in and kind of concern is around availability, right, energy security, right?  So if we if we, if we don't, if we can't necessarily, you know maybe we don't.  Our attacks don't result in, you know, release of material or anything, but we could put the thing off off grid, right offline. | | |
|  |  |
|  |  | P3 |  | Denial of service. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 244 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | And you know, it's blackouts or or or that sort of thing. | | |
|  |  | P3 |  | So that I think I saw something the other day that there's there's been a major outage on a telecommunications system in Ukraine, right?  So, you know, God forbid that we ever get to that sort stage, right?  But there's sort of real concern is, you know, I would be, it's like, well, there is these, you know, the likes of these nation states or whoever has some sort of latent capability, you know that sat within our critical infrastructures and you know that's waiting for the opportunity you know the right moment to be applied. | | |
|  |  |
|  |  | P3 |  | And I think that kind of that, that sort of Internet ification, let's say, of industrial control systems that are underpinning all of our CNI is, is, is, is, is something that's you know on its way and and well well underway I think which has sort of implications from a I think from a risk point of view. | | |
|  |  | P3 |  | So you know those sorts of things are slightly worrying, right?  And and it extremely difficult to detect, right.  And so yeah, those those are the kind of nightmare scenarios, I suppose that were that we would be worried about, I suppose, yeah. | | |
|  |  | P3 |  | You know, there's a lot of talk about using sort of generative AI mean it's not necessarily images to improve things like social engineering.  And in in this sort of space, then sort of maybe more on a kind of technical level, there's a whole class of attacks to control systems around manipulating input to them. | | |
|  |  | P3 |  | And and if it's, you know the the sort of issue with with, if it's a cyber, if it's a cyber problem, you know the major question is to what extent is the system trustable thereafter, right?  Can we just simply switch it back on again?  Probably not, right? | | |
|  |  | P3 |  | You know, how do you go about determining that you have sort of trustworthy systems after after the fact.  It's a kind of a major, major issue.  Like, have you really found all the compromise systems?  Do they still have some latent capability?  You know what I mean?  And and kind of those sorts of things that are more about sort of response and resilience in a sense, yeah. | | |
|  |  |
|  |  | P3 |  | You know, if you if you have an organizations that has some sort of risk management program, risk assessment, governance, risk and compliance program, a major component of that will be the sort of application of cyber threat intelligence of different sorts threaten to other. | | |
|  |  | P3 |  | I might be wrong, but I don't think privacy really features too much. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 245 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | The idea is that you you sort of adapt your you know your posture and your risk appetite based on the nature of the prevailing threat. | | |
|  |  | P4 |  | But I imagine you're going to see with this sort of technology, you can see a certain amount of encroachment purely cause of this technology readiness and also because it's certification readiness is very, very low.  And you know the you in order for that certification redness to go up, you're gonna have to have the ability to engineer systems that the the to do this. | | |
|  |  | P4 |  | And one of the things that I remember speaking when this is all when Stuxnet was actually happening and I was speaking to people who were who were working at these plants and they said, have you heard about Stuxnet and went?  No, no, that was just something we should sort of worry about.  And you know, we'd, we'd ask them.  What would your security you know?  Are you worried about, you know, attackers trying to come in and corrupt cool PLC to try and make your trying to make it do things you shouldn't do?  And they went no. | | |
|  |  |
|  |  | P4 |  | Actual threats and types of threats that we can't easily share with people, but at the same time, there needs to be assurance against it.  So you in a way you need to be able to.  Someone needs to be able to develop so.  So create software by by design, develop engineer, maintain it, et cetera against a threat that we may not actually be able to tell you about. | | |
|  |  | P4 |  | I one of the concerns I've got is around advance if we advance let's say a technology path to quickly such that in automation is taking control without people really understanding the implications of that.  Uh, and you get something bad happening because people don't don't understand what automation was supposed to do.  That that sort of worries me a bit.  And that and that's and that is as you described as a social technical problem, it's not simply an issue with the technology, but the history of all the courses that led to that, that instance to the happening as it were.  UM, safety is a big concern for us.  Very big concern.  I mean, traditionally our our team was probably more focused on safety than security and now it's about 5050.  And I think that's that's probably gonna be more of an that. | | |
|  |  |
|  |  |
|  |  | P4 |  | So | | |
|  |  | P4 |  | You know the sort of morachi the Maroochy Shire attack, but you know, people didn't really think about that when the infrastructure Moroka share MRO's MAR double OC, HY, if you just Google it, it's like considered like the seminal attack on on water systems. | | |
|  |  | P4 |  | Plants are just overloaded water and ends up waste.  Sewage ends up in the sort of river.  So that sort of things, you know, and that could that could cause harm. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 246 of 316 |  |
|  | | | | | | |
|  |  | P4 |  | You you could cause harm because they're they're worry was actually if you know much about water courses, the removal of so much green space means that a lot of water now floods into now actually goes into sort of drains.  And you know if if you get a lot of heavy, if you get a lot of heavy rain, you get wastewater treatment path. | | |
|  |  | P4 |  | Well, not really.  They kind of isolated systems, you know, I mean you you you could cause harm, but you know, you really would have to go out of your way.  And why would you wanna?  Why would you want to attack this particular wastewater treatment plant with with clean water is a little bit different with clean water.  The police are a lot more alerted into them, but you know, a typical sewage plant. | | |
|  |  |
|  |  | P5 |  | So let let's just take AI or digital twins right now if if people wanna use that technology to help the advanced reactor world for good purposes, great.  But from a security perspective, how do you trust back to the trust?  How do you trust that that digital twin hasn't been manipulated by a cyber adversary to give you the wrong results?  How do you not know that if you're using AI to make decisions to run a reactor that it's not, it didn't make some weird?  Connotations on something and says, hey, today I'm going to operate totally differently. | | |
|  |  |
|  |  | P5 |  | So that's really what I was talking about earlier was the blended attack.  Umm but yeah, so that's what we're trying to stop is usually the sabotage.  Bottom line is high consequence events, whatever those may be.  You know, if you're in the pharmaceutical business, you know you don't want an explosion, right?  You know, so you're gonna protect against explosions if you're in the financial districts, you know, obviously the integrity of your data.  You want it to be, you know, full integrity there and not come in the next day and find out you have 0 balance, right or worse a -, 1,000,000 pound thing or something. Right? | | |
|  |  |
|  |  | P5 |  | That's | | |
|  |  | P5 |  | If we stick with nuclear then it would probably be some form of sabotage.  Or or from a nuclear nonproliferation side, a theft of nuclear material.  And those are the two top ones.  I think that I would be focusing on umm, because you need, you know, safety to the public.  Of course, from a sabotage perspective and then the nonproliferation, you don't want dirty bombs and everything else going out there. | | |
|  |  |
|  |  | P5 |  | And especially when you talk about 5G though, now that maybe is outside of internal, so there are even more questions I would have if you're going up to satellites and back or not so and how that will work? | | |
|  |  | P5 |  | Yeah | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 247 of 316 |  |
|  | | | | | | |
|  |  | P5 |  | So | | |
|  |  | P5 |  | So I can tell you in the current reactor fleet, I'm sticking with nuclear right now because I don't have as much visibility into the other sectors anymore.  However, there is so much pressure being put on them, not only from vendors wanting to sell their products, but from the efficiencies that these new products are advertising, especially when it comes into outage control maintenance or they can walk around with a tablet, you know wirelessly and do their procedures and do their maintenance and just different walk around things that they do in the facilities that are wireless infrastructure would be very cool to have, right.  But there's they're up against our regulators, you know, and some other things where historically they've just said no wireless.  But I think even the NRC for us is potentially looking at what those risks are today compared to five or ten years ago and seeing whether or not they can lift any of that in certain circumstances or places. | | |
|  |  |
|  |  | P5 |  | And the other thing I guess I would just add as as you're an engineer as well is safety is always number one in nuclear, right?  And so, because we are now using so much digital technology for even our safety systems and our safety related systems, I really, really, really hope that the safety engineers understand the cyber security consequences and not only that, but they incorporate cybersecurity requirements into their designs.  And so that's where that cyber informed engineering comes in.  Is that idea that engineers need to fully be aware of cybersecurity?  Not necessarily experts they can call in the experts, but they have to be thinking absolutely and all their designs about cybersecurity. | | |
|  |  |
|  |  | P5 |  | I mean that may not be as dramatic or anything or maybe it wouldn't shut the whole industry down, but it's certainly would put everyone on pause.  It would cost a lot of money for people to say, Oh my gosh, these guys got into this nuclear plant in France.  We better check all of our nuclear unit solving our country to make sure we're not susceptible to the same thing.  So it's going to cost some money for sure. | | |
|  |  |
|  |  | P5 |  | So and so you you're particularly vulnerable from the point of view that it it wouldn't take a disaster to cause a huge actual impact. | | |
|  |  | P5 |  | Uh | | |
|  |  | P5 |  | Primarily I could say you know misoperation and some incidentals to someone typed in the wrong whatever, but primarily from a malicious perspective. | | |
|  |  | P6 |  | I mean the individual windmill is not critical.  But if I have 1000 of it and all of them have the same control software and I do an attack on the control software, then I can control thousands. I can also again attack the whole state so and I believe just because the malicious actor in this critical infrastructure is not yet well understood, well researched, period enough. And that's the reason why the impact is higher. So the threat is higher and it's more critical to look on this than the accident side. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 248 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | There is no producer which doesn't need additional data to improve the efficiency of his production process to to manage the the the supply chain, whatever it is that one needs at the future one meets weather data to improve his accuracy machine the other need other dates to compare his production data. So we are starting to exchange data very much in this machine context.  Very much also in the private context as personal human beings, either to create big data applications.  Look, I don't know a situation on streets. We don't need individual data, but we need many data. That's or we create AI, whatever it is of the behaviour analytics of people. So it's everybody produces data and we are shifting it around and also for the critical infrastructure. However, we will define it. So for metric providers, PowerPoint power generators. | | |
|  |  |
|  |  | P6 |  | Due to the digitalization and connectivity.  And using services and all this stuff.  Any IT system becomes more complex, so we are increasing dramatically complexity. Of course we are outsourcing a large extent. So for the stakeholder becomes easier because I'm outsourcing it to a cloud provider to service provider of course. But outsourcing doesn't mean that I get rid of the security responsibility so. | | |
|  |  | P6 |  | Then | | |
|  |  | P6 |  | And when we now accept as a threat model that we can discuss about philosophical way of political systems and human beings, there are plenty of threats out there which we see every day now on on the TV, there are always other people from crime to terrorism to state actors which will use.  Those vulnerabilities in our great infrastructures that we have very complex systems. So in Europe, we are answering now with increasing regulation and laws like NIST two and the Resilience Act. I think I believe it's a, it's a huge burden on the manufacturers and suppliers.  But I believe it's necessary that it's done, otherwise we will end up in a big mess. But nevertheless the question is, are we able to manage it? I mean, just having a regulation or law is something, but you have to enforce it, you have to.  The manufacturers to be able to implement it, we do not have laws that somebody's paying fines. We have lost the system's become more safe and more secure. So the question is, do we have the know how the people, the tools to build the system even we have laws out there to put the system much more resilient. And I would say I said before as a summary when it's even a management summary that we have from infrastructure to communication this data level now. | | |
|  |  |
|  |  |
|  |  | P6 |  | The the the sign process the the the at the very beginning already should take into account the potential threats and risk and then you're building the start of building the system according to it. You know just implementing it and then let's see and somebody else will sort it out and allow the IT organisation which doesn't have the knowledge to know how the people, the money and the tools should then protect the system. It doesn't work. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 249 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | I would say we are still building today IT systems that we have learned 30 years ago. We write code and then we put it together. I think this has to be changed fundamentally. We have to find new ways of building systems and testing systems. So a keyword will be by design. So we should we should securely by design safety and security by design. So we should think about architectures having tools supporting us how we are designing system.  Where our data so the architecture is understood, the system can help me and say OK can help me by the risk management if you do it that way. At the end security it's all about risk management. I will not answer the tools can help the engineer how to put the system from scratch that we've tried to prevent as much as possible. Vulnerabilities, wrong architectures, wrong system decisions. It will mean a higher cost at the beginning.  But it will decrease the cost at the end for testing and verification and all that we are doing today and we'll also have more resilient systems and this is not yet there in any kind of, I would say public organisation or large critical infrastructure operators and that's the challenge that they have. | | |
|  |  |
|  |  |
|  |  | P6 |  | Functioning of the system without bias and could conform. So how can we test and verify and validate AE algorithms? So that's also a new research field which started I think 10 years ago which started 10 years ago.  It's not mature at all. We need competence all over the world. So the question is, are we able from mechanically point, if you're really to master the EI technology by this mean, not just applying them, that's everybody's doing, that's easy.  But I'm asking exactly. | | |
|  |  |
|  |  | P6 |  | And on the other side, you have applying the EI in a more general context when when when personal data is involved, how can we ensure? | | |
|  |  | P6 |  | The data is the data already influenced and so there's a new mechanism how to deal with the secure system and thus I would say by far we are discussing this perhaps in the research world at the high end side. But I would say that's I cannot prove it. That's a belief that the state-of-the-art of knowledge and know how and abroad it scenario in the real world is not at all there. | | |
|  |  | P6 |  | They have much better problem. They are filled with the much simpler problems. The basics I would say, which we even would claim as an issue which is not at all a scope in my research agenda, but on the market. The big money is spent out there for consultancy to do the basics. I would say they are the high genius, the hygiene, dirty, the hygienic level and the Iit's through the basics. There has nothing to do with research. These are issues which were defined already 20 years ago.  But can the manufacturer afford it? That's the supply chain problem. If the supplier cannot do it to find a network operator will will get a bad solution. So that's the supply secure. The supply chain problem. I think that's the challenge with especially European manufacturers and suppliers will have. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 250 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | Energy Network operators, telecom operators, the definition of critical infrastructure, a government network, whatever it is, although they will use data, they are transporting data. So it is the biggest issue how to be solved. This data platform of the future where some economical systems of course will have strong impacts and the physical hardware storage data for example, that's not easy. Not everybody can do it in a cellar. So we have to have some kind of.  Concentration. But the question is it's just a first second concentration. What we have now also the data that the MINISM is it also the business and the control and all this stuff and so on this. So we have a speed of implementing, it's going very quick, the markets and the businesses, technologies developing. So that's a little bit of mess. Nobody knows exactly what to do. It's very easy to buy that. That's the threat for me.  To buy half price from China.  And to get services for free from duress because that's a big model of Google and Co, I give you the service for free, I can use the data and people don't understand it. That's the biggest issue. I would say that's that's on the one hand, the biggest challenge of course, when we go a little bit more in detail, it depends on when we come to this safety element, when we are in power plants and if you say critical infrastructure, more production facilities or safety where safety relevance.  Is plays also a role of course.  When we want to apply now AI on it, we have the big issue of how can we apply the advantage in the.  Possibilities of AI solutions in the safety context. So that's a big question mark which has to be worked on. How can we control at the end the black box AI or how can we implement AI models in a safety critical system? On the one hand. | | |
|  |  |
|  |  |
|  |  |
|  |  | P6 |  | So a classically I would say hybrid called hybrid threat where the the the media domain is combined with with online attack on the certic infrastructure and then you have a mess. | | |
|  |  | P6 |  | That's one of the problems that we have no understanding of greater infrastructure and when we have one platform where the whole world is on it like each, I don't know where is not. It's a very powerful communication platform and the algorithm behind is now defining who reads the information, who gets the information, who is applying it and when we go one step further, those this person which is controlling the platform has a more and we see it every day with.  We asked them. Elon Musk is masked behaviour behind it. We see he is now partnered. He is part of providing and influencing even the the result of a war. Unbelievable. Just because he has a private infrastructure which he can provide or not provide. You see that's coming back to my first statement. Individuals are became already very powerful, which in my old days 10 years ago, we were just on the state level.  And there is also changing. You see this. | | |
|  |  |
|  |  | P6 |  | We give it for free to the cloud provider, but that's that's all for the moment. | | |
|  |  | P6 |  | If dates are doing it unbelievable and even poorer states in the world will do it because they cannot afford it and this becomes now a big mess. So the big question is now how can we deal? | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 251 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | And everybody from private to industry, even to public, is using these cloud infrastructures.  And losing the whole serenity completely, that kid could not be the future. We are there at the moment. I don't believe that this will work from the business models will not work, but also from principle call IT security point of view. So the so the the, the the data's around The Who who owns the data who controls the data to build business on it but also to use it in our call it democratic systems it will not work if we completely give up.  The way how we control the data, that's the biggest challenge now how to deal with it.  I would say at the moment in industry is very active and we're talking by non privacy relevant data. OK let us build system and let us try to build marketplaces. The other side of the world still claims that's that's not important for us or we try to prevent. We do not want to have it because it's dangerous and we have all this, the whole public world, everything. But it's for me critical infrastructure.  Classically, in broad terms, we are not part of it, but at the same time, we use the big cloud providers and we give out our and when we lose our data sovereignty, that's unbelievable. So that's a completely mess of understanding, I would say. So especially because we have all these privacy concerns in our systems, we have to find new means.  And just saying do we are not doing it but but after after having said this we are doing it because we use Microsoft or Apple or something like this and we have done it. | | |
|  |  |
|  |  |
|  |  |
|  |  | P6 |  | And then you mentioned when I come to cybersecurity, I think.  Also, a very general statement.  It is true for any IT systems, but also of course also for critical infrastructures. | | |
|  |  | P6 |  | Yeah, there is potential threats from a quantum computing point of view for the encryption. I think this thread is serious. There's a lot of money is implement and a lot of sponsors are there to build such quantum computers. It's not yet there, but I imagine that this will be feasible. Human beings can do it. So we have a quantum computer there and then.  Lousy existing asymmetric encryption is under threat, and since the whole world is based on this, this threat is there. I see it very serious. We had. I mean, I'm also active in there. I'm biassed OK, but I think we have to think about it. How can we build next generation encryption just because it could not be that the whole world can read our data exchange, so we have to find means plus quantum encryption QKD. There are technologies out there? Which technology?  Finally, will be the successor in the global market. | | |
|  |  |
|  |  | P7 |  | How much you know how much of our, let's say, telecoms network? No, not not to to come to how much of our telecoms network need to be?  Survivable if you like.  In the event of a of of a global of of an attack from a from a foreign state actor.  To maintain. To maintain safety, you know, it's all all these things are not quantified. | | |
|  |  | P7 |  | So let's say that they they that that the CNI part of the CNI falls under attack that starts taking parts of it out of operation.  What? What intensity of an attack should the CNI system be able to sustain? | | |
|  |  | P7 |  | Yeah, I think I think we covered it as part of a of a previous point that yes, technology can can help the the defensive, but they can also help can also help the the offensive.  Yeah, I mean I yes, we just we just need to depending on you know, who who's interests you each of us represent.  We we have to to work and stay. Stay one step ahead. I mean that. You know, I don't think there is other any other resolution to this. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 252 of 316 |  |
|  | | | | | | |
|  |  | P7 |  | I mean, I'm sure there is. There is also there is also the the there is also always the the other viewpoint that you know, no, no, no we're we're staying as as much isolated as as we can.  You know are are sort of very good physical security also secures us from threats from the digital. I'm not saying it's wrong.  I'm. I'm just. I'm just saying that there is there is a risk of of missing something because because there is lots of things in systems that are changing.  They're getting they're getting more complicated. I mean, you know, did. | | |
|  |  |
|  |  | P8 |  | If you ask me, I say well, it keeps you up at night. I'm like, I'm seeing all these things. Either people don't see it or they see it, but they don't care, even though they care. They don't want us in the same field exam because we are very different people as I than they are. But we need to talk. I think lack of cooperation have I feel right. I know. I see so many things because I wasn't really prepared, but lack of cooperation between human factors, people, psychologists and the behaviour scientists and cybersecurity engineers and managers, really. Who is looking into all the CEOs of the C OS or whatever.  This is keeping my fit now, lack of talking if you ask me. Thank you. | | |
|  |  |
|  |  | P9 |  | Supreme individual sort of thing, actually. What you really care is that is is the banking system secure and resilient against all those sorts of attacks. So our financial records and our and our payment system and those sorts of things, they really do need to be protected in that way. I think they're already considered to be critical national infrastructure. But yeah, I do. I do remember when I was working on this very briefly in Cabinet Office the the realisation that critical infrastructure started as what do we need to recover from a nuclear strike. | | |
|  |  |
|  |  | P9 |  | The economy and finance, so many of the services and systems and economic mechanisms that we use today are now running on a data infrastructure that could fail every. So the network and everything else, their information model matters. We've got interesting conversation with somebody about Central bank, digital currencies and whether they need to be secure against quantum crypt attacks. And the challenge of course there is in a cryptocurrency or processing time is your transaction time. So you don't really want it to be very secure because that costs a lot of compute. | | |
|  |  |
|  |  | P9 |  | OK. There so that the meat, the information domain that's created or the knowledge domain, if you like in this created in this information space that's now digitally enabled is not a free and fair space? | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 253 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Safe Space to Coordinate between Organisations** |  | | | | | |
|
|  |  | P16 |  | I mean, you use the term negotiating something. You know, it's the the comments, you know, when you when you leave under a a comments system you know we you have to jointly agree with all the other users of the comments that you're not going to over exploit you're going to be and I think this is the kind same kind of.  Configuration where we need to be able to discuss and then to agree and then if we can't agree together, someone has gonna step in, has gonna to have to step in and probably the state and to say no. Now if you can't agree it's it's better if you agree together without enforcement or without and you coercion because it's very often introducing it's on emergent effects that are very often and desirable as well. But if you can't agree for a reason or another then I'll step in but.  Let's try to have a joint.  Discussion or negotiation among reasonable people or stakeholders to ensure that we understand how this interconnectedness is impacting everyone and how we can address it. | | |
|  |  |
|  |  |
|  |  | P16 |  | so that's making sure that we generate at the system level.  A way to regulate not only individual decisions like my decisions, but also the emergent effects that kind of negative emergent effects that are not my fault directly I I have got no I'll intent against you. It's just that because I'm not incentivized or not regulated, I'll keep on doing what serves me when I should also kind of maybe be made aware of the negative impact on you. | | |
|  |  | P16 |  | And we so we we need a even to be able to to know who to phone you. You need maybe to have like.  A A platform of trust from which we can communicate to each other. What what I am doing to you without necessarily kind of wanting to attack you. But what my decisions are doing to you and try to solve it together. So we need to develop.  For us, where we can discuss this and we can try to fix it together.  So that the overall ecosystem stays healthy. | | |
|  |  |
|  |  | P9 |  | If we can take collective ownership of that information space by representing ourselves properly and solving the collective action problem in the digital domain with the way that we've solved it in society, which is democracy and institutions, we can get the right institutions in that space, then we can take control of the information domain. I think we can fight that battle of ideas in an honest way, and from that we'll come a much healthier, happier and safer human society, one that isn't being led into destroying the environment through negative externalities and through and all that other good stuff that comes on. So I think I think those problems I talked about, you know big, they are solvable and the the roots, the root to solving it are the seeds that are taking root, as I mean are planted in there already. Those are the right mechanisms. But we're not using them in the right way. | | |
|  |  |
|  |  | P9 |  | So we really need to start to grow up and have a conversation conversation that says if you need to know something and I need to know something, we're talking information. Am I. Am I going to facilitate that exchange through giving you access to data?  And that's those are then two separate lines of activity. | | |
|  |  | P9 |  | And there's a difference between security and privacy and these other things, but basically that paradigm of information sharing, we can break that. So that information exchange is the norm.  Then complex systems can be managed at the information layer rather than at the layer where they physically interact with each other, and that gives us the ability to to solve a lot of these complex problems much more quickly. So that's that's one solution I would drive after that really quite hard. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 254 of 316 |  |
|  | | | | | | |
|  |  | P9 |  | In that information sphere there is an exchange of ideas and it needs to be nourished. It needs to be encouraged, it needs to be nourished, and it needs to be led, and it needs to be led in a noble spirit, by by people who are just encouraging the fact that things are said, you know, and I disagree fundamentally. Fundamentally, you know, with what you've said. But I would die in a ditch for your right to say it becomes that kind of behaviour that perpetuates.  And we need institutions and processes and practises that support that | | |
|  |  |
|  | | | | | | |
| **Safety Ignores Security** |  | | | | | |
|
|  |  | P11 |  | That doesn't actually say that quite, but you know when you read it and you think, hang on, what's going on there.  So that's why I make my comment about having cave and the O rings and all of that stuff. That's what worries me that one day someone will say, well, how could you possibly think this? | | |
|  |  | P11 |  | It's separate. So what it means is when I talk to.  And by the way, it's where I come from, so I'm hugely critical of the people who have, you know, that I've I work with.  What happens is the.  The safety engineers I work with abdicate responsibility, and if you read the safety standards and I'm I'm on a couple of committees and such like and I've reviewed one for railway, another one for nuclear, another one which is general, and they all suffer from the same problem as I see it, the safety standard says line one. Assume the security system is perfect and don't worry about it. | | |
|  |  |
|  |  | P11 |  | I really despair of the way that the world has created this profession called cybersecurity. | | |
|  | | | | | | |
| **Scandal** |  | | | | | |
|
|  |  | P11 |  | I think the.  Biggest concern to me, the thing that does keep me awake a little bit.  It is the headlong rush to get the benefits to to take the benefits of using complex digital technology.  Without really appreciating the risks that come with it, and setting aside some of those gains, some of those improvements in efficiency to pay for the protections. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 255 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | The IT it takes something like that to make people stop and say, well, how did this come? How did we come to this? I actually sent an e-mail to a colleague in NCSC saying something along these lines, like particularly the safety security thing. What causes me real anxiety is that at some point and I'll, I really will have retired by then. There will be the equivalent of the O rings or the OR the the Nimrod scandal.  And people will say.  How did we come to build industrial control systems in this manner?  Didn't we know? | | |
|  |  |
|  | | | | | | |
| **Secrecy Hampers Development and Response** |  | | | | | |
|
|  |  | P20 |  | we've just come out of this whole COVID pandemic where our ability to deal with COVID was severely affected, in my view, by a lack of Chinese transparency about what was going on. If we have a similar sort of scenario around AI.  Not transparent, you know, just as the Russians initially weren't transparent about the Chernobyl accident, how will that affect our ability to deal with the major crises in the area of cybersecurity or AI | | |
|  |  | P4 |  | But that is a feature of our of of this particular of this particular set sector. | | |
|  |  | P4 |  | So we have knowledge of.  Actual threats and types of threats that we can't easily share with people, but at the same time, there needs to be assurance against it.  So you in a way you need to be able to.  Someone needs to be able to develop so.  So create software by by design, develop engineer, maintain it, et cetera against a threat that we may not actually be able to tell you about.  Well, no, but but.  But to be fair is this is no different from security in in general, right? | | |
|  |  |
|  | | | | | | |
| **Secure Software Hardware by Design** |  | | | | | |
|
|  |  | P11 |  | Well, it isn't really. I mean, one of the solutions I think to the observability and the complexity problem is to make our systems less complex and more observable, but they then cost more money.  Unfortunately, you can't do that additively. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 256 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | You have to do it from the beginning at the point of design. By making these requirements.  You could say they're non functional or whatever functional requirement, but putting them in as part of the requirements for the system that you're building.  But I think we just lack the language. I think we lack the awareness.  So people aren't doing it, and and therefore perhaps what does concern me is that we are rushing headlong to build systems.  That at some point in the future we will discover weren't built well enough. | | |
|  |  |
|  |  | P20 |  | the security by design trend is a is a good and important one. I'm a bit sceptical about whether it's going to really take hold as I've said, but I mean that's at least it's the right principle in my view. | | |
|  |  | P3 |  | So things like this and then they did sort of develop this kind of implementation guidance which basically takes the engineering the V engineering lifecycle like from requirements to all the way through to access to decommissioning and each of the sort of steps in the engineering lifecycle, they kind of look at each of these principles and think about OK watch what are the questions that an engineer should be asking themselves in order to make the yeah. | | |
|  |  | P3 |  | Yeah, kind of work a little bit with some folks in, in the US and and and they the there's a DOE kind of initiative called Cyber Informed engineering.  Which is sort of, I think, gathering some momentum and getting some interest.  And that is really about sort of how do we make engineers on the one hand sort of aware of the cyber security and give them sort of essentially the core of it is principles. | | |
|  |  | P3 |  | Around sort of cyber informed engineering, you know and then you know it's sort of it is perhaps a little bit obvious to us maybe is sort of sort of computer scientists or whatever, but if you're an engineering this person. | | |
|  |  | P4 |  | Maybe what we should be calling ourselves, we should be calling what we call software engine is based is something that something like high integrity software engineering because people might not be passionate about building things for like water treatment systems, but they do want to build autonomous cars or drones and these sort of things.  And some of these things are actually high integrity systems because of what they do. | | |
|  |  | P5 |  | In safety as well, correct and and again it comes back to, you know, the adversary needs to understand, especially if they get into the operational technology side of what is the physics behind what they're trying to do.  And back to the Cyber informed engineering.  That's one of the core things too, is that we want engineers to think about the physics side with the security, so that even if an attacker got in through all your controls, the physics won't allow something to happen. | | |
|  |  |
|  |  | P5 |  | Air gapping is good and that is a security control that I would recommend. | | |
|  |  | P5 |  | And so, because we are now using so much digital technology for even our safety systems and our safety related systems, I really, really, really hope that the safety engineers understand the cyber security consequences and not only that, but they incorporate cybersecurity requirements into their designs.  And so that's where that cyber informed engineering comes in.  Is that idea that engineers need to fully be aware of cybersecurity?  Not necessarily experts they can call in the experts, but they have to be thinking absolutely and all their designs about cybersecurity. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 257 of 316 |  |
|  | | | | | | |
|  |  | P5 |  | And so if we are going to support these new technologies, these new advanced reactors, I really see that remote calms is something that has to be immediately figured out one way or the other because we haven't operated like that before.  Umm, we're operating in these big reactors that everything is right there locally and we don't have to do these remote things.  And so that opens. | | |
|  |  | P5 |  | And that opens up to, you know, outsiders in between the reactor and the control room, which may be Colomiers away, you know, anybody can now the physical protection is very different than posting guards or whatever at a facility.  So I think that's where my #1 push would be.  Is that remote communications? | | |
|  |  | P5 |  | So I guess that was more be my top ones for right now that I'm thinking about. | | |
|  |  | P5 |  | And one of the recommendations is to make it as simple as possible to perform only the function that you need it to perform of the system.  So for instance, you buy a programmable logic controller.  It may have two or 300 functions that it's capable of.  You basically configure the five functions that you want it to do for your process, and then all of those other hundreds are there.  If an adversary gets into that PLC, they potentially can enable those and do things that it wasn't designed for.  So our push is, if at all possible, remove all those other hundred functions out of that PLC, if that is possible.  The bottom line is you only want the system to perform the functions it's supposed to | | |
|  |  |
|  |  | P5 |  | You know, there's just, yeah, random base.  So I I would be looking at the security of all those support technologies I guess and including wireless, you know wireless has to be one of those top ones too because everybody wants to use wireless, it saves a lot of money, you know, cabling, trenching, those things. | | |
|  |  | P5 |  | And I agree, the more complex provides a greater attack surface that the adversary has at their disposal to come up with all kinds of scenarios. | | |
|  |  | P5 |  | So yeah, interconnected.  That's why we talk a lot about defensive architectures and segmentation, where you segment these things so that no one can get to those critical systems.  So yeah, that's definitely a big one. | | |
|  |  | P6 |  | we are still building today IT systems that we have learned 30 years ago. We write code and then we put it together. I think this has to be changed fundamentally. We have to find new ways of building systems and testing systems. So a keyword will be by design. So we should we should securely by design safety and security by design. So we should think about architectures having tools supporting us how we are designing system. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 258 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Secure System Testing** |  | | | | | |
|
|  |  | P5 |  | Is a simulation, so I would just say that make sure that it as part of your research that you get to the point where you do your test and evaluation on a real real equipment real facility, real whatever, to prove it out. | | |
|  |  | P5 |  | It I think it's more because I think it's more because people who write simulation can't simulate exactly everything in the real world.  That's why I think it has to be in real hardware. | | |
|  |  | P5 |  | I do think though, that whatever methodologies or research type activities that you perform that ultimately it needs to be proven in the field, it needs to be proven with real equipment, real architecture, real test bed, whatever it's gonna be.  I think you have to show what your research results are to prove.  This is why it works. | | |
|  |  | P5 |  | It's not just necessarily that the hardware might operate differently or not.  It's just that you will find things that you never accounted for in your simulation.  The weather.  Do you do you accommodate the weather in your modeling and simulation?  And you know what?  Maybe you didn't know that the weather has an electromagnetic interference on your COM cables or whatever, right?  So that's where real world has to be at the end of your research, I think somehow. | | |
|  |  |
|  | | | | | | |
| **Shift to Preventative Medicine** |  | | | | | |
|
|  |  | P13 |  | it's not just diagnosis. I think it's again it's it's about prediction and prevention and being able to know what the right intervention is and when the right time to make that intervention is. | | |
|  |  | P13 |  | I don't know. I mean, people have been talking about for quite a while.  And maybe that time scale more like 20 to 30.  I mean, I mean, I think back where we were 30 years ago, that would have been what mid 90s.  Yeah, maybe I'm being a bit optimistic then.  Oh, I don't know though. Mid 90S was just the start of the Internet era, wasn't it, really. Yeah, I'd, I'd, I'd go with 30 years potentially. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 259 of 316 |  |
|  | | | | | | |
|  |  | P13 |  | this, this, this represents a fairly fundamental shift as well for how we deliver healthcare and it goes back to what I was saying about shifting changing from a reactive model to an eventative model. Our system isn't geared to do that. That's not how it works. It's there to, to rescue you when something bad happens. | | |
|  |  | P13 |  | Yeah, and and and this, this shift towards.  Away from a reactive healthcare system to preventative system is often cited as the only way you will make healthcare scale.  Into well in the next 1020 forty years because.  We can't just keep treating ageing populations with multi morbid conditions each time they they they something bad happens to them and.  That's really a driver and it's an economic driver of supporting the health system, supporting hospitals. And so that's where it directly links into actually, how do we support this critical infrastructure or you have to shift towards a more preventative model. | | |
|  |  |
|  | | | | | | |
| **Small Nuclear Reactor Risks** |  | | | | | |
|
|  |  | P3 |  | You know, how do you go about determining that you have sort of trustworthy systems after after the fact.  It's a kind of a major, major issue.  Like, have you really found all the compromise systems?  Do they still have some latent capability?  You know what I mean?  And and kind of those sorts of things that are more about sort of response and resilience in a sense, yeah. | | |
|  |  |
|  |  | P3 |  | Sort of sort of.  Equation has changed.  Then there's sort of risk shifts little bit to be more about nuclear safety like you have this thing in the middle of nowhere with not many staff an increase risk of somebody sort of stealing material. | | |
|  |  | P3 |  | And if you're using digital systems to support remote surveillance, physical protection systems, or this kind of stuff as part of a blended attack, then theft of material is becomes a bit of an issue.  And then the other kind of sort of potential shift in and kind of concern is around availability, right, energy security, right? | | |
|  |  | P3 |  | And and if it's, you know the the sort of issue with with, if it's a cyber, if it's a cyber problem, you know the major question is to what extent is the system trustable thereafter, right?  Can we just simply switch it back on again?  Probably not, right? | | |
|  |  | P3 |  | And you know, it's blackouts or or or that sort of thing. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 260 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | Most of the scenarios that I've kind of thought of that we thought about in the nuclear space, the kind of, yeah, it's some controlled or uncontrolled trip over the reactor, right? | | |
|  |  | P3 |  | Uh, how readily can we determine what's the root cause of that right and then sort of be able to respond effectively?  I could, I think if you know outside of just doing the, you know doing the the the trip or whatever it is that just to disconnect to contain the issue.  We sort of really need to understand what's happened really quickly. | | |
|  |  | P3 |  | Not necessarily a nuclear safety thing, but basically some trip that puts the thing offline, which causes a sort of significant power outage because you know, from what I understand, I'm not nuclear engineer or nuclear operator.  But you know, it's not like you can say, oh, well, trip it and then we'll just switch it back on again.  You know, we're talking a few days before before we can bring them back online. | | |
|  |  | P5 |  | If we stick with nuclear then it would probably be some form of sabotage.  Or or from a nuclear nonproliferation side, a theft of nuclear material.  And those are the two top ones.  I think that I would be focusing on umm, because you need, you know, safety to the public.  Of course, from a sabotage perspective and then the nonproliferation, you don't want dirty bombs and everything else going out there. | | |
|  |  |
|  | | | | | | |
| **Smart Sensors and Digital Twins** |  | | | | | |
|
|  |  | P11 |  | Operational technology in the CNI remains in the level sort of 1 and 0 area, but that's where a lot of the smart sensors are coming in. Smart sensors and actuators. And so you could regard that as being IoT. | | |
|  |  | P13 |  | And by exposure I mean things in the environment that may impact on your health, like cumulatively over a long period of time.  May impact you and again that's really down to the sensors connectivity.  Essentially, but I suppose what's also interesting about this connectivity and this almost real time stream of data about conditions, it enables us to start using things like prediction.  To understand potential when your health conditions are going to deteriorate.  Drive a really general prevention, because if you know you're about to deteriorate, it's often something you can do in a long term condition so. So that's actually kind of the next thing that's coming and it's almost there. And again, that's what about by fairly conventional technologies, sensors, networking increase computation. So I think that's where we are and.  When I mentioned things like protection actually leads into a lot of the I stuff you say because a lot of it is around prediction models. But then of course you've got lots of things that are diagnostic models that take in images and tell you whether you've got a brain tumour or whatever. And so so we've kind of got all that.  So that's what we are. So do you want to project forwards a little bit more? | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 261 of 316 |  |
|  | | | | | | |
|  |  | P13 |  | Other things we are still starting to see and this is making a major change to our health systems operate is the direct connection of patients into the healthcare system through the kind of communication technologies.  So here I'm thinking about.  Smartphones, wearable devices, IoT type sensors. Let's give us a more holistic picture of an individual in their free living life.  And if you have, say for example a long term condition, we're able to monitor that long term condition as it changes and fluctuates.  We're also able to do things such as understand people's exposure. | | |
|  |  |
|  |  | P13 |  | And you basically take all that data and you train a transform model and that would actually do the prediction for you because you just give an example of. Well, I'm a patient with such and such and such a disease, watching the next treatment day and that autopasset captures all that knowledge and percentage you what should come next. So you can see that that could be a potential direction as well. | | |
|  |  | P13 |  | the concept of digital twins.  Which kind of tie? All those things that I just mentioned together into kind of a more coherent framework. So if you imagine, for example, a digital twin of everybody that represents you as an individual.  Knows your susceptibility to disease through your genome, understands you, or represents your complete medical history or complete exposure to things. You can start to predict your lifetime risk of developing different diseases and start doing prevention. And so that's kind of the evolution of where we are now and people are starting to think about that and wonder how you might make that possible.  Some of the interesting things around digital twins are potentially potentially, if you were then to network those things together.  And actually what you'd end up with is a population of digital twins that could communicate with each other, and you can start to imagine.  Well, actually I'm looking at you and I don't know what the best treatment is for you, but I could go and look at all the other digital twins that look a bit like you and see what happened to them and use that to inform the next treatment. And so you you end up with kind of this distributed knowledge of all of medical healthcare and.  You can you can see how that would develop. | | |
|  |  |
|  |  |
|  |  | P15 |  | So biggest game changes I think is is going to have to be something around like data sharing and situational awareness and understanding.  Because that is always a problem.  Is is getting information from where it is to where it needs to be and knowing how to interpret that for what has happened in front of you.  AI could be will certainly be useful in terms of.  Being able to summarise huge amounts of data potentially.  That in in a short amount of time. | | |
|  |  |
|  |  | P17 |  | we're at the point where we're telling national highways, you know, you're going to have to change your model, your operating model, you'll you'll you'll sock operate model.  And these are the new technologies that you're gonna have to on board. So when you onboard these systems, they're gonna have to be different. You know, there's gonna be a different process to what you're used to today.  And and I've touched on other points on it as well in this call, which is you know, you know you go from, I don't know, consuming millions of events to trillions of events. You know, how do you, how do you have platforms that can handle that? But you know, you and correlate across, you know, not just ten sets of data streams, but a billion data streams. You know, how does the correlation work and stuff like that? It's.  Right. So yeah, so we've got, we've got some papers we've been looking at to to help. So I can you know something related to sort of highways, something related to rail and maritime. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 262 of 316 |  |
|  | | | | | | |
|  |  | P17 |  | So you know, there's a lot more of that sort of starting to expand in in that particular area. And I think that would be the same for rail and maritime as well. So very much transportation sort of area. So there's definitely a lot more kind of edge sensor and edge computing which which is classified as IoT really. I think that's definitely an area that we're we're going to see more of a drive into as well. And I think if you sort of coupled that, even if you not necessarily C and I, but I mean you already start to see body tech you know like in you know.  Interjected chips and stuff like that into human bodies to interact with machines. | | |
|  |  |
|  |  | P17 |  | With the movement in the sort of digital twin space, there's there's a massive move there at the moment and it's really in its to early stages at the moment, but there's lots of funding and research going in that into that sort of space | | |
|  |  | P17 |  | you I don't know whether it's a linear kind of curve at the moment and whether that sort of starts to turn into this sort of exponential rise in in five to 10 years time. But with the amount of computational elements that we're starting to now. So this this is the itot convergence and and realistically we should start to say I TOT and IoT convergence really we should add the IT in there because that's going to fuel it. I think there's going to be a sort of blurred line between.  Because because at the moment the problem we have in industry is there's a real lack of understanding of what assets we have. | | |
|  |  |
|  |  | P17 |  | think there's going to be this kind of weird sort of.  Yeah, bit like a like a snooker shot. You know, where you play a ball of three or four different cushions before you hit the actual shot you're you're trying to look at. And the reason I use that term is that I don't think you're going to get necessarily the direct throughput change in the OT sector on CNI just by saying, you know, we need to do more protective resilience based stuff and therefore you need to go and buy this product or this solution and and stick it in type thing. I don't think that necessarily is going to happen tomorrow or the next few years.  There is obviously a drive towards that kind of change, but I don't think it's going to be.  You know, drastic and and and and a high curve, I think what's going to happen is there's going to be a bigger influx in knowledge about the systems that they have, whether that's through data collection or more exploratory sort of analysis of their systems and networks. And then using that data offline or or or sort of kind of decoupled in a way to inform business decisions and those business decisions then drive business cases to drive the changes in, in the system infrastructure and whether that.  Means then that there's gonna be an improved, you know, cyber resilience by putting in the solutions themselves or whether that's gonna be a case of, you know, we will stick stuff in like IO T Edge kind of infrastructure because you know we've we've taken something out of our network. We've analysed it whether that be real time or offline, whatever we've made some informed decisions, we've seen a business case which is going to drive better efficiencies. I think that's the way it will work rather than saying you know there's credible threats now.  Or there will be tomorrow. You need to kind of start protecting the edge and work your way backwards into your infrastructure. Basically, I think it's going to kind of work in a sort of backward prong way. | | |
|  |  |
|  |  |
|  |  |
|  |  | P17 |  | you know in the automation industry and the the highways, you know you got edge to edge like vehicle to vehicle, vehicle to person. So wearables, you know, talking to to cars basically.  Vehicle talking to infrastructure so the smart motorways, you got vehicle to vehicle. So car to car and you've also got vehicle to cloud and vehicle to telco SO45G. | | |
|  |  | P24 |  | believe IoT it it has helped a lot in terms of utilities, which it's a critical service.  In societies using I I did a research last year on.  A. The application of IoT specifically for smart sensors and how they could.  Improve the supply and demand of demand of energy in. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 263 of 316 |  |
|  | | | | | | |
|  |  | P24 |  | Houses in like all around the world | | |
|  |  | P3 |  | You know the use of cloud potentially kind of associate that also with you know the use of digital twins, which is a sort of a kind of a hot topic if you're in that operational technology space.  Sort of telecommunications, right?  Which is sort of not really a thing that people.  I've I've sort of thought about too much in kind of nuclear before, and then things like uh, you know, sensor networks and in particular kind of wireless sensor networks or wireless instrumentation and control. | | |
|  |  |
|  |  | P3 |  | So one of the sort of issues with this smars and microreactors in particular is that you don't have an awful lot of space for for equipment.  So that sort of pushes sort of people to think about kind of wireless sensor networks and stuff like that because you don't have kind of maybe as a support, I mean again, so this is all ideas that at some point need to hit regulatory reality. | | |
|  |  | P5 |  | I hope it's not controlling the reactors, but I hope it's only informing them and there's conversations about that. | | |
|  |  | P5 |  | they're talking about, of course, the use potentially of AI, machine learning, digital twins.  These are the buzzwords. | | |
|  | | | | | | |
| **Societal Harms through CNI Failures** |  | | | | | |
|
|  |  | P12 |  | The thing is with power plants and water they could produce a lot of.  You know unrest. So we saw with the colonial pipeline ransomware incident, you know there wasn't a gas shortage actually there was just a panic that produced the gas shortage.  Or like the ransomware didn't produce a gas shortage directly produced it indirectly. | | |
|  |  | P13 |  | People's behaviour is changed by things that they read that are not necessarily true.  And so you can imagine that those kinds of things could be more manipulated by those technologies more easily.  Just because they're potentially more convincing. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 264 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Software** |  | | | | | |
|
|  |  | P4 |  | The the work we did around Athens was motivated around the idea that all this novel technology is going to come along.  It could end up on an air platform, and it's gonna need to be certified.  Now if you look at software certification, it's not just about testing. | | |
|  |  | P4 |  | It's sociotechnical, but it's also technical as well. | | |
|  |  | P4 |  | So not just software assurance, but security, safety, human factors by that usability and how all this stuff comes together because somebody bad might want to exploit that. | | |
|  |  | P4 |  | We're talking about platforms here that will be around for maybe four or five decades, which actually and if you look at a lot of critical infrastructure, these are long lived systems | | |
|  |  | P4 |  | It's not just about verifying the software we care about validating the software.  We care about security and safety, and we all secure about whether the people operating it and maintaining it have sufficient knowledge. | | |
|  | | | | | | |
| **Software Hardware Service Supply Chain Problems** |  | | | | | |
|
|  |  | P11 |  | I think it's the way that we write software is a concern to me. It's.  I saw an article in the IEEE which I haven't read, but really resonated it said. Is this the year that we did finally deal with bloatware?  What it's talking about, I think, is the tendency to. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 265 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | I wasn't distinguishing between hard between hardware and software particularly, I did mention it a couple of times, but I wasn't. When I was talking about complexity.  I see the boundary between them being quite difficult to distinguish in terms of their contribution to to complexity, because for example the integrated circuit.  May have is it 2 billion transistors and has been has been laid out by a CAD Cam system that was written in C + + 20 years ago. | | |
|  |  | P11 |  | to stand on the shoulders of predecessors in writing software. In other words, I will just incorporate this library. Well, it worked for me last year, so it'll work for me this year. Yeah. Where did it come from? I don't know. | | |
|  |  | P11 |  | it introduces the kind of complexity which is anathema to the kinds of things that I'm looking for. | | |
|  |  | P13 |  | we have seen these kinds of things destructed by protests. So I'm thinking back to the fuel protesters, we had one must be like 15 years ago now that actually brought supply chains.  Down and that was relatively easy and thing to do actually. I mean what they did was barricade a fuel fuel depot and the whole thing came to halt.  So there's that kind of thing.  Other things that might affect it is where these things are manufactured.  So if you look at so the Pharmaceutical industry, it's a global industry.  Manufacturing takes place in various different locations around the world. It could be political threats there. That meant actually, that could disrupt your supply chain. | | |
|  |  |
|  |  | P16 |  | Software that we that are used very broadly for you know free that you get from Itab and other places and repositories of.  Bits and pieces of software, then they're they're being used for those major.  Uh. Uh umm.  Control for critical infrastructures and then suddenly we realised that we depend on.  Crappy programming by done by a single person that everyone assumed was very safe but no one bothered to check, and then we end up like the heart bleed or incident or and then my concern would be that instead of discovering it and being able to fix it without anyone having had the opportunity to leverage it for an attack, we we find it about we find out it during an attack and after our systems have collapsed and.  And we end up in situation and you know our societies.  Are not ready to absorb.  Some types of collapses of certain systems. | | |
|  |  |
|  |  | P16 |  | So what we found is that the banks are very worried, for example about their.  Ability to guarantee that they will keep on being able to trade even during a crisis, because now they don't control. | | |
|  |  | P16 |  | Computing systems directly anymore, but they rely on 3rd party providers.  Of which they know very little about, | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 266 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | the legal sector, it's very interesting sector because it's not very tech savvy in the sense that usually.  Legal professionals. They tend to stick very much to tradition and to, but it's it's surprising how critical they are actually to the operations of the critical infrastructure sectors, because any company doing a merger and acquisition of another company has to.  Go through a a a a legal service provider that has access to their most important secrets. Their most important financial statements, and the legal sector, so holds the secret because of the cleaned you know the the the the attorney-client privilege and all of that. So they hold secrets.  The most important secrets of the biggest companies in the world, not not being very sophisticated at technology and keeping.  Under wrap, like the police or intelligence community. And so the the attackers are very knowledgeable of that and and and the target. And I know I know I speak of experience because I've acted as an expert witness in a number of cases that were never, never went to court because no one wants to hear about that or to air that kind of weaknesses but.  Those are cases of.  Billions of dollars in in, in fraud and secrets being stolen on the massive scale. | | |
|  |  |
|  |  |
|  |  | P16 |  | but also the open source. | | |
|  |  | P21 |  | But it can be an existential threat, that sort of business interruption. You can't manufacture, you can't produce, and so on. | | |
|  |  | P21 |  | So I think an incident would sort of be a major CNACNI supplier.  And then either.  Either someone who's already designated CNI, but I think the the greater worry for me is someone in their supply chain who isn't actually CNI, but then effects all kinds of CNI businesses as a result in the supply chain. So I think someone like a defence contractor or someone who does sort of logistics. | | |
|  |  | P21 |  | . If it's A/C and I supplier that deals with something like that that I think would be quite quite worrying. | | |
|  |  | P21 |  | there's examples of like the past and providing the CCTV camera for your manufacturing side. Someone coming in with a track regularly or like sort of people who are providing services to their CNI provider. And if those are affected and they could, they could possibly provide CCTV to not just one CNI provider but to several right. You could sort of see someone providing CCTV to like.  UK army bases or something like that?  And so where someone who is in CNI and perhaps sort of has fallen through the cracks of a lot of service, security regulation is impacted. But because the way ransomware attacks work, so the a secondary victims of someone experiencing a ransomware attack in their supply chain often faces the exact same harm that the 1st order victim does, except for that they have less information about what's going on. So that kind of makes it even worse. | | |
|  |  |
|  |  | P21 |  | If your pension number is being stolen or your.  What's it called? Your national security, not your national.  What's the number code that you're? Yeah. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 267 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | And then I think something else that would very much worry me is if it's.  Biometric data that's being stolen or genetic data that's being stolen.  So that certain kinds of data that would be particularly worried about. | | |
|  |  | P21 |  | That thing isn't so, but at the same time, then you couldn't deliver fresh produce because you could no longer rack it up. You can't deliver it. You can't distribute it. The the supply chain doesn't work because the manufacturing stage is no longer work. Then a lot of your food goes off because you can't seal it. Those kind of things.  And we've seen in COVID and sort of even if you like, we live in Glasgow and there's a snowstorm every once in a while, you see how people panic. If there's the idea that there isn't enough food or like, there's something, even if it's just limited options in the supermarket, people can not spread. You can imagine something like that.  Yeah, I think something like that. Similarly, if you have a supplier of oxygen to hospitals or something like that, I'm not sure, hospitals certainly CNI supplier of oxygens could be a pretty niche. | | |
|  |  |
|  |  | P21 |  | there's only one company who does like food packaging or something like that or wrapping freakin stuff.  Then maybe food, logistics and supplies, or C and I, but wrapping. | | |
|  |  | P21 |  | Yeah, that can be. You can get a new one. Like if you can't easily get a new one, but if you really have to, you could get a new one, whereas your DNA date on your DNA and sort of other biometrics and that you can't change and.  It would sort of, yeah, quite worry me. | | |
|  |  | P3 |  | Yeah, you know, so, so, you know if if you target a kind of, you know, I don't know distribution system operator directly or or a nuclear facility directly.  That's really hard, but if you tag in one of those suppliers, it's maybe a little bit easier and he gets you away in right? | | |
|  |  | P3 |  | Yeah, cause yeah, if you if you have libraries that are part of your that are critical to your business continuity or your societally critical infrastructure that's provided by GitHub, then you, you know that's that's important, right. | | |
|  |  | P3 |  | So if you go back to the kind of smart grid kind of area, you know, there's sort of, you know, you to use a horrible American expression like mom and pop type organizations with relevant, you know, you know, I'm obsessed with security, but with relatively low security maturity or whatever kind of having sort of quite relatively critical interfaces to just sort of critical infrastructure operators.  So yeah, I would say it's generally great and I think that's also evidenced a little bit. | | |
|  |  | P3 |  | There's been sort of the people, the organizations that were targeted and then to the best of my knowledge like this to sort of extends that skull quite significantly to to other other actors.  And I and I guess this sort of the thing as well, that sort of really hot in this area is supply chain, right?  And so that the criticality of the supply chain is is sort of there.  And so the these critical infrastructure operators known, do they have an interface to critical infrastructure? | | |
|  |  |
|  |  | P6 |  | But can the manufacturer afford it? That's the supply chain problem. If the supplier cannot do it to find a network operator will will get a bad solution. So that's the supply secure. The supply chain problem. I think that's the challenge with especially European manufacturers and suppliers will have. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 268 of 316 |  |
|  | | | | | | |
|  |  | P7 |  | Did the network operate or something, let alone national infrastructure, right? Did did the network operators that you know were were buying chips and routers from from foreign country manufacturers like five years ago would would know the situation that we would be now and talk about all the supply chain | | |
|  |  | P9 |  | I mean, you talk about the fact that the compute layer is now CNI, when it wasn't before and and a bizarre range of online services.  There is a there's a. There's a risk pattern emerging to come back to this adjacent possible idea, and the fact that innovation is connecting things together. People are building services on the back of really, really flaky previous services and then at some point it suddenly becomes desperately important and you realise that underneath it, you know, there's a fantastic XKCD cartoon | | |
|  |  |
|  |  | P9 |  | . Basically, if you want to use any kind of genuinely advanced technology which is running in your laptop right now and in your smartphone and in your car and everything else, anything within the last ten years or so, cutting edge technology, it will have been made in the fab, in, in Taiwan at TSMC, which is why this is. This is a deliberate ploy. By the time these government to make sure that they were protected from the Chinese by the Americans, by securing.  Something that the Americans can't afford to let go. | | |
|  |  |
|  |  | P9 |  | That's economic statecraft for you of the highest order, massive respect. There's only one company in the world that builds the machines that TSMC can use. They're the only people that can use them. But the only people that can build them is a company in Holland.  And because it's very, very advanced photolithography on the thing, and the only company in the world that can build the optics that enables those machines to work is in Denver. So we tend to look at that and go. All right, we can. There's a chain there that makes that makes sense. But for many of these other things, we don't know where it comes from. We don't know where the bottlenecks are. They're shifting and changing. They're going, they're crossing all sorts of borders. So the old fashioned idea of economic statecraft around how I'm going to manipulate supply and demand and and and interface between nations in the trading nation, that's now.  Unmanageable in terms of its complexity, which is interesting. | | |
|  |  |
|  | | | | | | |
| **Speed of change** |  | | | | | |
|
|  |  | P18 |  | Given the nature of like the dynamic nature of the kind of cyber world, whether you know just be updates or cybersecurity update needs, then you need a strong strategy in there to say that, OK, we'll only update when the.  I mean and and these things happen and how vulnerable does that make you in between, you know? So there's, I mean, these aren't these are new issues to to but they are but they're but they're issues that become more prevalent because of the increased use of digital.  Or the reliance rather than misuse of of digital systems, I mean, but digital systems on the on the opposite, are we going to be positive as well? Digital citizens on the opposite opposite side allow you a lot more information. They the diagnostics have got a lot more advanced. So you can try and identify or rather than try you can identify.  Where things may be going wrong.  Earlier and deal with it in a proactive way, so it's not, it's not all bad. You know, there's there's.  They can. They can do more complex functions in a simple or more cost effective way, so you know there's lots of benefits to them as well. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 269 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | There's also a guess the.  The rapid nature of change as well.  Umm. Which you know, all of these can be flipped around to be a positive as well. You know the the rapid nature of change means that.  It becomes difficult to.  Maintain you know, as an engineering maintenance.  A good example of that is.  The cybersecurity you know, updating your cyber arrangements is is a classic example that if you need to prove a piece of software is doing its thing.  That takes a long time to do that, and a lot of testing if then you recognise as a vulnerability with it, and then you make a change to it, then you have to do all that proof again. Yeah, so. | | |
|  |  |
|  | | | | | | |
| **Standardised Off-the-shelf Software** |  | | | | | |
|
|  |  | P11 |  | The increasing migration of of IT type technology down from let's say level 4 into 3 and two so.  Increasingly, you see Windows based platforms being used for HM is and.  Engineering workstations, et cetera, it's becoming much more standardised stuff than network. Technology is much more standardised, so the types of switches.  And and so on and so forth. | | |
|  | | | | | | |
| **Standards - guidelines** |  | | | | | |
|
|  |  | P20 |  | Yeah. Well, I think, I mean what, one of the things that.  I'm concerned about in terms of software development is.  You know, this idea of sort of rush to release of software, particularly AI platforms, because you want to get ahead of other commercial operators, but also other countries. So you have, you know in my view open AI releasing ChatGPT in a in a way and form that I don't think was entirely responsible where there were numerous vulnerabilities which were observed only after it was released.  And I think you know the this rush to release this idea of, OK, well, we won't. We won't do sort of all that much in the way of proper security testing or risk assessment of the software will just get it out into the into the world and let you know Crowdsource that and and let others figure out what the vulnerabilities are. I don't think that this is a particularly responsible.  Process for software development in the context of AI technologies, and I think it's historically been the same for cyber. We're caught between wanting convenience and wanting ease of use, but but not having very secure products. So I think this has been a feature of the political economy. If you like, of of cybersecurity.  So I think that there's some concerns about software development and how the the the regulation is put in place around.  Commercial competition over new products, which might create risks, including for national infrastructure and then layer on top of the commercial competition. You've got the geopolitical competition where producers of software are saying.  Don't regulate us because if you do, China will beat us to general AI. | | |
|  |  |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 270 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | I mean the the NHS has learned the hard way or the UK has learned about the energy, cyber, but you could certainly envisage scenarios where the cybersecurity standards are just not that high for someone who doesn't have that reporting requirements or doesn't get.  Certain support from NCSC in the 1st place, or they might not do that essentials or something like that, and we see even even. | | |
|  |  | P7 |  | Or they will tell you that you know, if you connect things to a network, you better use you know.  RJ45 connectors and make sure your network is is segmented, but this is as far as they will go. You know we don't we don't know I mean.  So let's say that they they that that the CNI part of the CNI falls under attack that starts taking parts of it out of operation.  What? What intensity of an attack should the CNI system be able to sustain? | | |
|  |  |
|  |  | P7 |  | So if you look at some, if you look at.  Different standards. You know, I'm thinking of 6483.  The calves that you see from NCSC and and other bodies cyber assessment frameworks.  And and and other standards when they touch cybersecurity, their their guidelines are very generic.  Very, very, you know qualitative, you know they will tell you you know, if you have systems speaking to each other then communication better be encrypted. But this is as far as as they as they will go. | | |
|  |  |
|  |  | P7 |  | How much you know how much of our, let's say, telecoms network? No, not not to to come to how much of our telecoms network need to be?  Survivable if you like.  In the event of a of of a global of of an attack from a from a foreign state actor.  To maintain. To maintain safety, you know, it's all all these things are not quantified. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 271 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Super AI** |  | | | | | |
|
|  |  | P9 |  | there's going to be a symbiotic relationship between human beings and their environment, just as there is today. And that environment will include super intelligent entities. What those entities look like will really challenge us. I think the botanists will have a better grasp on it than the zoologist because the sense of self and identity will shift.  We tend to we tend to assume that identity relates to a single isolated physical body, because that's the way that we do things. I am not the same as you. We are separate and we also look at things like speciation and go well. Humans are cleaning up horses, so we know how the world works until you look at it in detail at the edges. Species is an abstraction which doesn't make any sense at the biological level. You can always find blur cases in between, particularly for the sort of non zoological higher order vertebras. But plants themselves, you can take a cutting from a plant and you can take it somewhere else and plant it.  And it will grow in a completely different physical form.  Genetically, it's the same plant. It's actually a piece of the same entity. It's like taking my hand and planting it somewhere and it grows into an octopus, and then you'd be cutting off the octopus and you bring it back and put it into my house and it turns into a clone of me. That's what plants do. And they communicate chemically in, in, in social structures as well as independently, the sense of self and the sense of identity that we hold around systems is all based on our understanding of animals.  These big systems are a lot more like plants. They're they're dispersed through the infrastructure, their complex ecosystems of information flow.  They're interesting synergies between the different parts of it, including humans writing material down and building the machines and putting the energy in. We have no idea how they're going to act. This is not going to be like Ian Banks. Drones. I'm me. That's my drone. We're separate people. That is an entry point into an intelligent ecosystem that does not make any sense to human being. OK, so once we're in that world, what do we want to be? Do you want to be tigers or chickens?  And the Tigers, tigers human beings tolerate tigers because we think they're brilliant. They're gorgeous when they're in the wild. We kill them because they eat our children, but we keep them in zoos. We keep them in, in, in cages because they're nice to have around and we don't want to lose them. But they're dangerous and we don't want too many.  Or we could be chickens, which bear no relationship to the original bird but are now the most. I think they're the most sort of populous bird in the history of birds ever. There are more chickens alive today than any other. All the other birds put together is because we like to eat them. | | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  | P9 |  | Because they're useful to us. I don't know what our future is with these entities, and it might be next generation. It might be 2 generations time, but somewhere down the line there comes a point where you're going your relationship in service to this wider information ecosystem that is now digitally mediated. Are you a tiger or are you a chicken? Are you a Centaur or are you a minotaur? And the choice we have is not P doom. This thing kills us. But what sort of symbiotic relationship do we want to have with this new information environment? | | |
|  |  |
|  |  | P9 |  | So human beings will be essential to this wider information mediation engine.  But we won't know what our functioning it is where we want to recognise it might not even recognise that it's intelligent because it's doing so at a level which just just beyond our comprehension. So there's a lot more, you know, I all of that sort of sounds apocalyptically. Oh my God, it's nightmare. It's like never will be delighted in the whatever the future is assuming that we survive the climate change crisis which the machine will hopefully tell us how to do.  But but it won't be the same as being a human being as we understand it today. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 272 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Supply Chains** |  | | | | | |
|
|  |  | P10 |  | And yeah, the interconnectedness around supply chains, but, but particularly the the sort of the sort of cyber connection here is is, is, is critical, absolutely. | | |
|  |  | P12 |  | I really think global supply chains are are leading the way of those things like chips. And, you know, now I just read an FT today that the US is concerned that China's going to dump goods because they have this industrial over supply problem and that that's going to disrupt a little. So these sorts of things are, you know, are, you know. | | |
|  |  | P13 |  | And I suppose you can look at things like supply chains.  And if you think about how, for example, medication is supplied and distributed, that's critical part of infrastructure. Same with things that are like PPE, for example, when you saw that through COVID. So I think I think that the whole supply chain.  Across the NHS that keeps it functioning is probably, yes, critical. | | |
|  |  | P16 |  | Some supply chains were very, very thinly, thinly spread and.  Almost collapsed they they've kind of managed to subsist and so I think what the pandemic showed is that some supply chains and some systems, they're very resilient and and you know, we switched instantly.  To remote work without.  Societies. So. So that's very reassuring. So that's why I sleep very well. I think that as a as a species, we we have a highly adaptive capacity that we'll be able to find fixes and solutions, but also we we identified some weaknesses in the supply chain that we deploy as developed economies and we rely on just in time. And I think that we should think a lot more about just in case and and and think and that's why my work now is.  Mostly on cyber resilience instead of cybersecurity because I think cybersecurity is the wrong.  Framework in the sense that it's kind of an impossible objective to achieve with this new technologies and these new risks. So we should actually try to be happy with cyber resilience. You know, if we can keep functioning, you know. | | |
|  |  |
|  |  |
|  |  | P16 |  | All organisations are using heavily, depending dependent on on cloud computing solutions. The problem is that when you have a financial so when you have a critical infrastructures are usually very heavily regulated.  And for a good reason, so that the regulators and the state ultimately want to ensure that they put in place systems to maintain high levels of reliability and we can have confidence in their ability to deliver critical services to to the population, what is not so heavily or so.  Meticulously regulated are those.  Cloud computing technologies, upon which those critical infrastructures more tend to rely more and more. So what we found is that the banks are very worried, for example about their.  Ability to guarantee that they will keep on being able to trade even during a crisis, because now they don't control. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 273 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | Complexity.  And very often by companies that come from very different sectors, from very different understanding of what security is about. And it's very.  Very sophisticated companies because of the levels of investment required and they're very hard for the customers to really know what's happening in those data centres and to really have a guarantee of their so. So I think really cloud computing would would be.  For me, the the really critical.  Component of of of those? Yeah, as a trend, it's something that it is really super important.  E-mail problem, yeah. | | |
|  |  |
|  |  | P16 |  | Computing systems directly anymore, but they rely on 3rd party providers.  Of which they know very little about, so it's easy for a bank to ask to see what's happening in the systems of their partner financial traders, because everyone has to abide by the same type of regulation, and so they trust each other. They know they have to operate, but then it's impossible to ask a financial partner institution to have access to their Microsoft.  Or IBM or Amazon cloud.  Services because those companies are much bigger and they say no, no, no, we just provide a service to you. Trust us. You know, we have thousands of engineers, so it's creating.  Lack of understanding of the the reliability and so the cloud computing. And now I think in the I think in the in the US the the the financial sector regulators are now asking submitting the cloud computing companies that service the financial sector.  To some high levels of oversight as well.  Saying that, if you want to enter this business with a financial.  Institutions, you're going to be part of the packet you're becoming part of the package now, so we're going to have to ensure that you deliver certain levels of services according to certain requirements. I think that the cloud computing, because it's introducing another layer of. | | |
|  |  |
|  |  |
|  |  | P16 |  | Software that we that are used very broadly for you know free that you get from Itab and other places and repositories of.  Bits and pieces of software, then they're they're being used for those major.  Uh. Uh umm.  Control for critical infrastructures and then suddenly we realised that we depend on.  Crappy programming by done by a single person that everyone assumed was very safe but no one bothered to check, and then we end up like the heart bleed or incident or and then my concern would be that instead of discovering it and being able to fix it without anyone having had the opportunity to leverage it for an attack, we we find it about we find out it during an attack and after our systems have collapsed and.  And we end up in situation and you know our societies.  Are not ready to absorb.  Some types of collapses of certain systems. I mean, we've seen it during the pandemic. | | |
|  |  |
|  |  |
|  |  | P21 |  | So I think something that has that kind of implication.  That pushes. I mean the UK has capable, it's called assert, a cyber emergency response teams, but the NCSE is good, but they.  There's also limits to how much they can do so if it's a coordinated effort that I'll matches. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 274 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | Provide like there's examples of like the past and providing the CCTV camera for your manufacturing side. Someone coming in with a track regularly or like sort of people who are providing services to their CNI provider. And if those are affected and they could, they could possibly provide CCTV to not just one CNI provider but to several right. You could sort of see someone providing CCTV to like.  UK army bases or something like that?  And so where someone who is in CNI and perhaps sort of has fallen through the cracks of a lot of service, security regulation is impacted. But because the way ransomware attacks work, so the a secondary victims of someone experiencing a ransomware attack in their supply chain often faces the exact same harm that the 1st order victim does, except for that they have less information about what's going on. So that kind of makes it even worse.  So that's sort of something that. | | |
|  |  |
|  |  | P21 |  | The one example we talked about in the context, someone, for example, who provides umm can can be hey, I want to say there's only one company who does like food packaging or something like that or wrapping freakin stuff.  Then maybe food, logistics and supplies, or C and I, but wrapping. | | |
|  |  | P21 |  | That thing isn't so, but at the same time, then you couldn't deliver fresh produce because you could no longer rack it up. You can't deliver it. You can't distribute it. The the supply chain doesn't work because the manufacturing stage is no longer work. Then a lot of your food goes off because you can't seal it. Those kind of things.  And we've seen in COVID and sort of even if you like, we live in Glasgow and there's a snowstorm every once in a while, you see how people panic. If there's the idea that there isn't enough food or like, there's something, even if it's just limited options in the supermarket, people can not spread. You can imagine something like that.  Yeah, I think something like that. Similarly, if you have a supplier of oxygen to hospitals or something like that, I'm not sure, hospitals certainly CNI supplier of oxygens could be a pretty niche. | | |
|  |  |
|  |  | P21 |  | I don't know whether they would. They would fall under the afternoon to could be other medicine. | | |
|  |  | P21 |  | Well, that's quite hard. So I think an incident would sort of be a major CNACNI supplier.  And then either.  Either someone who's already designated CNI, but I think the the greater worry for me is someone in their supply chain who isn't actually CNI, but then effects all kinds of CNI businesses as a result in the supply chain. So I think someone like a defence contractor or someone who does sort of logistics. | | |
|  |  |
|  |  | P21 |  | People who make all the chips, and there's one factory in Taiwan that makes every chip in in the used in telecoms or something. Yes, yes, yeah. | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 275 of 316 |  |
|  | | | | | | |
|  |  | P22 |  | And so there are movements in terms of responsibility and authority and ability to control and assumptions. And that's one of the dangerous things because the IT guys are caught between a rock and a hard place.  They used to being able to say, you know, my guys have developed as we've tested it, it's OK. I mean that's the picture.  But that is no longer the reality. You know, the reality is you're dependent on well, we we were looking at this for the we were wondering whether to suggest the US federal government's approach of an espon, you know, software bill of materials.  And that the guys who?  Of operational it guys were saying can be stupid. Yeah, most most sensible organisation have got probably like at least 50 to 100 different suppliers built up in their system.  You having an S form would just add to the complication. I mean it wouldn't do anything because you know you've got to keep up with update cycles of each of them.  And even if it's BeenVerified at Level 3.  By the time it goes to level 3.109, do you have to re verify it? It's just, yeah. And so that's another of the reasons why we pulled back to say, impact measure. What's important, measure the failures, find out how to fix those. Yeah. Look to look at real life, not a theoretical approach. | | |
|  |  |
|  |  |
|  |  | P22 |  | And so talking to the chief architect, I think is called at British Airways.  One of the big problems was finding a backup cloud for some of the places where he had to have data centres because obviously it's a wide worldwide network and it goes to some, you know, goes across the Middle East and so on and.  But they had built into all their thinking that would be a resilient cloud, so the applications assumed everything was going to keep working, so he couldn't. He wasn't, didn't have the budget to build into his applications, ways of checking if things were failing because the assumption was the cloud would keep working. | | |
|  |  |
|  |  | P22 |  | but you know, we drew a little picture at the beginning of our study saying, you know, here's a A Venn diagram also. This is the, this is the software.  In use in the UK, this is the software developed in the UK and so in improving, yeah.  Slightly overlapping but and so in terms of improving the productivity of the UK, keeping the cnir, yeah, it's, you know, it's not within our control.  Because you're buying, you're buying software that's on the open market. You have it or you have not. And cloud computing is in that category and. | | |
|  |  |
|  |  | P23 |  | Lot it's it's become a major concern.  I I also work for a law firm.  We represent only startups.  Or formal advice at the moment is not to accept investment at all from China.  It's too risky and it can essentially get you into trouble with federal regulators.  And there's nothing you can do if that the Cepheus process of its triggered.  There's nothing you can do it.  The issues pertaining to any data, not just things, but also any data that is sensitive, which is soon soon people are gonna figure out that all data are sensitive. | | |
|  |  |
|  |  | P23 |  | Supply chain criticality as being, you know, a major issue and and not handled very well in law and procurement either.  It did have you come across that one at all. | | |
|  |  | P23 |  | And | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 276 of 316 |  |
|  | | | | | | |
|  |  | P24 |  | Yes, yeah, yeah, I did that mainly for, like from the project management side, but I also contributed in workshops.  Related to the more technical aspect.  So for example A1 project that I contributed significantly in the risk assessment was an environmental and social impact assessment for a railway in Columbia. So it was thinking about many different possible scenarios like people stealing material materials from the road or also.  Trying to steal the copper, I think it's name of the catenary, so that led to many impacts also, not only for the operation of the train but also social impacts. So it's like trying to have.  A wider view of the whole system, not just like I need this to run and to give me money, but also how does it affect?  The other elements in society.  People, environment and supply chain of other industries as well. | | |
|  |  |
|  |  |
|  |  | P24 |  | Try to manage or mitigate risks that would lead to the road being closed. Then, for example, in Columbia we don't have much railway systems, we we don't have basically at all. So all the fried transport goes through road infrastructure and when one Rd is closed because any. | | |
|  |  | P3 |  | And I and I guess this sort of the thing as well, that sort of really hot in this area is supply chain, right?  And so that the criticality of the supply chain is is sort of there.  And so the these critical infrastructure operators known, do they have an interface to critical infrastructure?  Well, no, I'm not sure.  No, is the right answer.  Maybe it's maybe. | | |
|  |  |
|  |  | P3 |  | Essential to the operation of if if these these sort of critical infrastructures that we have, and so, so just to give you a bit of an example like in the nuclear sector, the UK civil sector are now doing a supply chain mapping exercise sort of like OK, who are our suppliers and then sort of looking at well if there's these sets are support you know they set of suppliers that are providing to the UK civil nuclear sector, what's the overlapping set, right?  And then all of a sudden we've got the set of organizations that turn out to be critical to the UK civil nuclear sector, because if they disappear for whatever reason, uh, we're kind of a little bit in a bad shape because. | | |
|  |  |
|  |  | P3 |  | Do you have the contract language in place where they're obliged to support you if something goes sideways, all those sorts of kinds of issues, so they kind of become essential to your business continuity.  And so I think people are just starting to wake up to this now as a sort of a bit of, you know, as a sort of significant issue.  And we're still very early. | | |
|  |  | P3 |  | You know the the huge issue you know basically like with supply chain you know a lot of it is around you know understanding your supply chain, who who, who are they, who are the you know you're critical suppliers you know, do you have a good set of communications to them in case you need them. | | |
|  |  | P5 |  | Air gapping is good and that is a security control that I would recommend.  However, we do have to move data eventually somehow through flash drives through supply chain you replace a part.  How good is the part that's coming in?  Did you check?  Maybe it has malware on it that comes in right?  Umm, there's lots of ways to bridge the air gap, but air gap is still one security control that you should probably should do if possible.  Yeah, it's a defense in-depth process. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 277 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | They have much better problem. They are filled with the much simpler problems. The basics I would say, which we even would claim as an issue which is not at all a scope in my research agenda, but on the market. The big money is spent out there for consultancy to do the basics. I would say they are the high genius, the hygiene, dirty, the hygienic level and the Iit's through the basics. There has nothing to do with research. These are issues which were defined already 20 years ago.  But can the manufacturer afford it? That's the supply chain problem. If the supplier cannot do it to find a network operator will will get a bad solution. So that's the supply secure. The supply chain problem. I think that's the challenge with especially European manufacturers and suppliers will have. | | |
|  |  |
|  |  | P7 |  | Did the network operate or something, let alone national infrastructure, right? Did did the network operators that you know were were buying chips and routers from from foreign country manufacturers like five years ago would would know the situation that we would be now and talk about all the supply chain and, you know, risks to because OK, we talk about national infrastructure and we talk about now energy and and and defence, but telecoms is is a very. | | |
|  |  | P9 |  | That's economic statecraft for you of the highest order, massive respect. There's only one company in the world that builds the machines that TSMC can use. They're the only people that can use them. But the only people that can build them is a company in Holland.  And because it's very, very advanced photolithography on the thing, and the only company in the world that can build the optics that enables those machines to work is in Denver. So we tend to look at that and go. All right, we can. There's a chain there that makes that makes sense. But for many of these other things, we don't know where it comes from. We don't know where the bottlenecks are. They're shifting and changing. They're going, they're crossing all sorts of borders. So the old fashioned idea of economic statecraft around how I'm going to manipulate supply and demand and and and interface between nations in the trading nation, that's now.  Unmanageable in terms of its complexity, | | |
|  |  |
|  |  | P9 |  | Yeah. So I think things, things that worry me.  The complex entanglement of systems around this technology, and let me take a few different levels in that.  And I'm I'm riffing on something I haven't unpacked in quite a while, so it's might take a while to reassemble.  If we look at the supply chain for these technologies, not just the digital technologies, but the critical national infrastructure which they enable.  It is very, very distributed and very poorly understood.  It's probably too complex to be well mapped, but we will continue to fixate on choke points in key stories. So one of the famous stories that's running out at the moment, thanks to Mr. Miller and his book chip walls, is.  The relationship between TSMC and I forget the name of the company in Holland and the company in Denver. Basically, if you want to use any kind of genuinely advanced technology which is running in your laptop right now and in your smartphone and in your car and everything else, anything within the last ten years or so, cutting edge technology, it will have been made in the fab, in, in Taiwan at TSMC, which is why this is. This is a deliberate ploy. By the time these government to make sure that they were protected from the Chinese by the Americans, by securing.  Something that the Americans can't afford to let go. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 278 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **System Complexity Increasing** |  | | | | | |
|
|  |  | P12 |  | it does feel that we've already reached a level of network size that would be pretty difficult for a human to reason about.  So I think we're past that Inflexion point. So then would there be some other Inflexion point where like even I OK, here's the way I would think about this question, right?  With these interconnection points I or with you know, this kind of general problem, that's like kind of graph complexity, right?  You rely on automated solutions to identify issues. I imagine that those systems have some kind of computational complexity, so you have to do some graph search. Is that how does that graph sort? Scale? You know, is it in NP? You know, I actually don't know about how these systems work in practise, but I think what you would want to do if you were trying to evaluate those questions like OK of these systems that are actually used to evaluate interconnection.  Are there any problems that are in NP, and if so?  When or how would we expect that to become a problem? Like at what point would we expect this to be impractical to actually compute? And then how are we going to deal with that if there's no good answer, then I would say yeah, maybe. But otherwise I would kind of my instinct on this, honestly, is like we're already there, like we've been there for maybe five years already. | | |
|  |  |
|  |  |
|  |  | P16 |  | It's just like the fact that when you have those interconnected interdependent systems and you have like a very autonomous tools now being developed to attack or to defend. So you have machines that are making decision just like in the stock market when you have an initial, you know, a tiny event.  Generating a cascade of decisions.  Decisions by, you know, in microseconds by.  Software that is trying to beat the crowd. | | |
|  |  |
|  |  | P18 |  | So yeah, that's complicated. That's gonna get even more complicated because of the diverse nature of of energy generation from wind, solar, you know, and little micro grids rather than, you know, big ends, big sectors or big spots of energy that was previously from large power stations. So that dispersed nature of of energy production.  Put a a stability issue on the on the National Grid. So if you use AI to try and help inform that balancing supply and demand, making sure that all the local factors are are taken to go into account even as a predictive tool to say, OK, what's the, what's the the sunshine going to be in next week the how much solar are we going to get, you know and all that sort of stuff. | | |
|  |  |
|  |  | P18 |  | So so you know to balance supply and demand for instance on the electricity grid? | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 279 of 316 |  |
|  | | | | | | |
|  |  | P3 |  | know it all started with this idea of having prosumers, right, that have some sort of interface to the energy distribution, the distribution system operator or the DNL is, I think the called here in the UK.  Then it's like sort of, you know, energy service providers of different source doing things like demand response and they sort of signal into you know basically there are kind of relationships between these entities to make sure that we have frequency at 50 Hertz voltage stays within a certain band.  You know, I sort of interfaces onto the energy market as well.  So they're basically the whole thing gets a little bit like I say, a little bit more open.  There are kind of more say programming interfaces or API's that that kind of exist to sort of realize this sort of vision and this in connect interconnected grid and then sort of there are kind of new communication protocols that are being used.  Some of these are sort of, uh, more Internet like in their kind of operation, which is a sort of departure, I suppose, from from the way that these sort of.  Systems operated in the past just to give you an example. | | |
|  |  |
|  |  |
|  |  | P4 |  | I mean to, to be fair, the military has always been about systems systems. | | |
|  |  | P6 |  | A very active globally in doing interconnecting the next group of the next market or group. We're connecting all our technical system so call it now industry for the 5:30.  Everything is will be connected with everything, so we are we are building this full connectivity. So that's for the moment we have to deal with the people connectivity. The next challenge which is not yet there.  Is this machine to machine connectivity, so that's still going on. The next element, which is the next decade, which I think is now crucial. What we are just starting globally is building on this technical platform. It is there now everywhere you have IT. So that's for mediaturization. It's a full connectivity. Everybody can in principle reach each other. We have connectivity and in each.  Moment. What? It's a sensor or a powerful computer. Whatever it is, we have a piece of software. So that's these. Two parts are now. That's what that machine machine can communicate. And all this stuff. So this system is now generating the platform of the new would say data economy, which is now starting. And this is not yet. No, no, no, even not completely. That's not yet understood at all. | | |
|  |  |
|  |  |
|  | | | | | | |
| **System Resilience Approach** |  | | | | | |
|
|  |  | P11 |  | we're going to.  Have to adopt some of the more sort of system theoretic type stuff that Nancy Leveson talks about.  Except in a way that's practical. Sorry, Nancy. In a way that doesn't require more hours than there are in the universe to model the system.  And for the safety people.  Stop focusing on random.  Unrelated, uncoordinated.  Mechanical like, you know, like Poisson function type, you know. Oh, oh, here comes another one failures which we can model from historical behaviour. Where's all the system? Is it systemic? Systematic anyways.  Where are the systemic risks? | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 280 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | My position is as a systems engineering problem because I think that it's.  The achievement of resilience.  In the face of adversarial action.  Or failures of of unusual nature because we don't have the history such As for weird types of censors or whatever.  Needs to be done in a different way than the manner in which we're currently teaching it. | | |
|  |  |
|  |  | P11 |  | I see security is being taught too much as an additive activity.  An existing system design.  Particularly one that has been through all the safety processes and has been deemed to be, you know, just just fantastic, that's just excellent. So now with your security nodes, please do whatever it is you do, but don't touch our system because it's, you know, because it's fine now we want to put it online. So we you'll probably want to put some do some stuff around it. | | |
|  |  |
|  |  | P13 |  | Or as a sad.  Compromise of systems.  I mean, it's quite interesting in a way in that.  Although you you think our health system in terms of the NHS is one thing, it's not actually one thing at all, it's actually lots of small organisations.  Under essentially the same it's almost like a franchise system in a way, and so there is quite a bit of resilience and independence between them. And I mean, if you look at, for example, when you have major incidents. | | |
|  |  |
|  |  | P13 |  | Such as train crash, plane crash, whatever. The system is able to deal with that by distributing casualties. Who need care.  Across the all the regional hospitals and so you know, I mean it does function quite well in that respect to those kind of critical incidents I think. | | |
|  |  | P14 |  | And to try and encourage that sort of system of thinking.  So yeah, it's got as the world gets more complex and more connected, | | |
|  |  | P14 |  | So that's just a question hanging there and I don't know if I know that 5G and there's there going to be A6 GI, guess there's going to be a 6G.  You're dealing with smaller and smaller cells.  And delivering.  And managing messages.  So that is a decentralisation in a sense.  And does that build more resilience? I guess potentially it does, but I just just asking the question. | | |
|  |  |
|  |  | P14 |  | Thinks about the systemic elements in it as well, and then delivers, develops mitigation a really effective risk management approach would be my number 11 recommendation.  Rather than getting fixated on a particular topic or theme or. | | |
|  |  | P16 |  | I think that as a as a species, we we have a highly adaptive capacity that we'll be able to find fixes and solutions, but also we we identified some weaknesses in the supply chain that we deploy as developed economies and we rely on just in time. And I think that we should think a lot more about just in case and and and think and that's why my work now is.  Mostly on cyber resilience instead of cybersecurity because I think cybersecurity is the wrong.  Framework in the sense that it's kind of an impossible objective to achieve with this new technologies and these new risks. So we should actually try to be happy with cyber resilience. You know, if we can keep functioning, you know. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 281 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | black start on the grid, you know, it's becomes really important and that and and that black start is you know how do we recover from a kind of mass blackout and kind of what's the time scales what's the process so that that recoverability I think is an important aspect. | | |
|  |  | P18 |  | the likelihood of failure of AI is 1. The likelihood of having a cyber attack is 1, and and if you think if you think about it in those those that those terms, you might seem kind of negative and pessimistic.  But actually it drives the right behaviour and the right engineering and the right kind of protection or whatever.  If you think Anna will be OK, then you think you can guarantee that you're going to get bitten. | | |
|  |  |
|  |  | P18 |  | So, yes, I am thinking about systems thinking and. And I'm thinking about it in both the traditional sense of systems thinking. So systems engineering, software engineering, that's sort of approach. But I'm also thinking about it in bringing in those human elements as well. And at Lancaster University, you've got the soft systems methodology that kind of.  Checklist developed, you know, so you know that that sort of thinking where you're you're looking at hard stuff as in physical stuff, but you're also looking at human behaviour around that as well and motivations to do things and and all that sort of thing. So it's not just a like a physical system, it's as you said.  The the kind of interplay of of people around that physical system as well, I think is important. | | |
|  |  |
|  |  | P18 |  | it's the ability to recover that becomes important so that if you, if everything's interconnected and so it starts.  Doing its thing its its thing. This often is you know very difficult to stop that propagation of the issue but so it becomes a function like the impact becomes a function of your ability to recover, to stop and recover. | | |
|  |  | P18 |  | I think we have to step out from that and think about whole system.  So if you're going to do something new.  Thinking about the consequences of failure.  And and you know and developing that. So you actually understand.  How the failure of the AI is going to propagate and result in whatever what the risks, you know, the likelihood of those happening, the consequences happening. But that's a whole system's view rather than just looking at the AI we tend we have a tendency to focus just on an AI, for example. But we've got a step away from that and think about the whole system.  And and its potential impact. | | |
|  |  |
|  |  | P18 |  | So, so when we think about physical things needed to be happening, we also think about procedures around there. And we think about.  Plant people and process so you know those three things in order. You know, an effective system.  Has plans aspects to it. It has the people aspects and it has process aspects to it as well. So so we do think about it in those terms.  Yeah. And the stuff that I'm doing again with offgem, you know, I'm trying to take a systems thinking approach into that. You know, when you're looking at especially on.  You know, I mentioned about kind of the impact of AI on society rather than national infrastructure. You know, that's very much.  A technology and people centred approach.  But then you know, in terms of national critical national infrastructure, you know the the markets can have an influence on that as well. And that's you know that the markets isn't a physical thing. That's that's people. | | |
|  |  |
|  |  |
|  |  | P18 |  | So we've got something really complicated or complex rather, and it's gonna have an impact on something if let's not, let's not just stop there. Let's think about the knock on effects of that. So yes, it's a whole system's view rather than thinking too narrow. Narrow. I mean, there's a limit, isn't it? Because you could end up with everything being the same problem. So. But, you know, thinking beyond the technology I think is important. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 282 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | Including the people. Yeah | | |
|  |  | P18 |  | And then and people motivation rather than rather than, you know, technical motivation and necessarily keeping the lights on, you know, it's it's all about kind of.  Personal motivations as well. Profit, those sort of things fairness. | | |
|  |  | P19 |  | Given that these systems are not not not that well protected, but the moment Charles, I think that more research is needed in the field to to, to design and and actually to after the fact.  I resilience into systems, could you?  You can't just start again and and and they'll just look from scratch.  So I think it's important to to use people, people from other disciplines to think about the the risks involved in no resilience comes at a cost, because with resilience, we're talking about adding redundant components and paths.  So the the these are are gonna cost and I I suspect that in the past systems and service providers have maybe been a bit reluctant to to add.  Yeah, costly resources like this, of course. | | |
|  |  |
|  |  | P19 |  | by Michael Ungar, who's a Canadian Researcher) resilience.  So this book called Multi Systemic Resilience, Right published in 2021.  That's that's what looking at right.  And what's more, it's all Open Access. | | |
|  |  | P19 |  | xxx  It's got this summation of several years of buying efforts on technical approaches to resilience, particular in the face of disasters. | | |
|  |  | P19 |  | And I think that that's important because I think some folks in the past have thought if if we if we build enough protection into systems.  Yeah, well, there.  But they were all right.  But you have to think about what happens when the world gets benefited.  Yes, you have to to think about the perhaps unlikely, but all too frequent penetrating of the cyber war.  What happens when the bad guys get in?  Yes, you've got to be prepared for that.  And that's about. | | |
|  |  |
|  |  | P19 |  | These systems may individually we have been addressed by different disciplines.  So yeah, there's there's a need for that.  The prosthesis.  Yes, impedance matching. Yes. | | |
|  |  | P19 |  | Also, by the way, humans there's sources of problem solving.  Indeed, really.  Because people who run, for example, utilities including telecoms, are themselves experts.  And what what does go wrong and how to fix the problems?  So the, the these these people can be valuable assets I. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 283 of 316 |  |
|  | | | | | | |
|  |  | P19 |  | That's about this resilience by design.  So, and what might resilience by design look like then?  Well, I I I think that.  Probably companies that are are designing systems instructs probably do some of the there's already yes, because they they have forums where they talk to users and they they tried to build the they tried to specify the software so that it will six.  You know what?  The users need what I'm saying is alongside of that, the you you have to think about the risks of things that will go wrong.  Probably you, you you know, you're you're deciding how much redundance you're redundancy to to fit into the technical parts of systems.  You have to think about how you you deal with the the likelihood of people be compromised or people making mistakes. | | |
|  |  |
|  |  | P19 |  | And of course, our cybersecurity colleagues are right.  They're working away on on how you make combat the the the attacks that yes that you have.  But I think some of them don't probably don't go far enough that that begun to talk about cyber resilience. | | |
|  |  | P19 |  | it's resilience that we care about it.  Yes, yes, we're still don't tell the building and the capability to detect problems happening to act fast, to recover it and that recovery and the recovery getting back to to normal services is very important. | | |
|  |  | P4 |  | Oh, knowledge exchange.  Literally, knowledge at I mean to me it is.  I mean, it could be my background but.  I you know the these are issues with square pipeline.  I've talked about it with too many people across different sectors, who have all said that it it's an issue.  So people, you know, within government, things think it's an issue.  People in our supplier base think it's it's in issue.  Complementary people in hardware think think it's an issue. | | |
|  |  |
|  |  | P4 |  | So so we have all these people saying too fast.  We have all these people saying too fast.  Sociotechnical needs to catch up and everybody's saying it's an issue, but they're not really talking to each other. | | |
|  |  | P4 |  | People in university, I think it's an issue, so knowledge exchange. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 284 of 316 |  |
|  | | | | | | |
|  |  | P6 |  | Whatever crisis disasters in natural disasters.  It was out there a little bit, but it was never priority in no state we didn't spend.  Enough attention to it priority as societies all over Europe, I would call it. It was out there. Researchers were there, Ng OS were working there, but we didn't make it serious enough. And and the private market.  Did not invest in this kind of resilience because it was not necessary and that for me the solution when we come to the end, I think from a cyber security point of view, but also from this resilience point of view that our society is is still working, we need.  All together as end user private end user, but also as a business user. So at the end it becomes systems and products will become more expensive also besides the good stuff.  I think we have to deal with it. We cannot, we cannot spare it. It has to become more expensive than the systems become more reliable, more safe, more secure and in a global perspective, I believe then also manufacturers and service providers are more competitive. But we are not yet there.  So this more investment in more resilient systems will be the solution at the end or one approach. | | |
|  |  |
|  |  |
|  |  | P7 |  | Resilience mentality. If you like that we need to protect, we need to have mechanisms in hardware and software in place that protect the operation of our systems and we need to accept that some of the resources and some of the of the electricity and some you know will go towards this. It's not, it's not going to be you know.  We we cannot, we cannot live without it. | | |
|  |  | P7 |  | We need to put effort into making systems.  All, all all computer systems, resilient and and what that means is, you know, beyond the sort of security by design, right. Which basically means having bound pointers that, you know do not do not do not 'cause memory leaks. I mean, OK, I'm I'm I'm. I'm half joking over simplifying it but.  The the point is that we we we we cannot afford, so we need.  Mechanisms to be there, always on and and protect.  Our infrastructures, critical or otherwise, but but obviously the critical ones.  Against things happening, so we need to do a bit of a mentality change from trying to prevent things from happen, to accept things, bad things will happen. But then we need to be to have the right mechanisms in place to respond fast.  And you know, minimise damage and return to a sort of normal operation level as soon as as soon as possible. | | |
|  |  |
|  |  | P7 |  | So this is this is definitely I think I think I think we need to do so you know, don't look at mechanisms like instrumentation, monitoring, service provisioning, don't look at them as as as overhead because that's that's that's the way we've been looking at them you know for the past 50 years if not if not more at least in the digital space where the fact the past 50 years you know I'm I'm not I'm not going to turn SNMP or Netflow on my router because it eats resources and then.  And I need to sustain line rate bundled.  I think in our I think in our.  Not so, not defence, but in our raid. The fact that technology becomes cheaper and you know, programmable silicon now being the same price as fixed silicon helps.  But but but I think beyond the hardware beyond the these kinds of developments, we really need a, a, a sort of. | | |
|  |  |
|  |  | P7 |  | But I think the the case one way or another will be established and we will need to move in, in an era where, you know.  The same way that you know, we design critical systems that depend on on computing to be to be safe, to be reliable, to be available. The same requirements there would be for cybersecurity and resilience. | | |
|  |  | P7 |  | Having, you know, having our our our systems and and networks embed this capability and I'm, I'm, I'm I'm I'm intentionally including.  Networks here because as I said, you cannot. You cannot possibly expect every individual system to be to have any sort of minimum standard of security, right? | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 285 of 316 |  |
|  | | | | | | |
|  |  | P9 |  | The real disasters and crises will happen, and we'll fix them and they'll happen and we'll fix them. It's the systemic, it's the, it's the system implications of that that are challenging, will we, will we survive the disaster and will be resilient to fix it afterwards? Or or will it fundamentally pivot our our society? | | |
|  |  | P9 |  | systemic fragility and it comes back to stuff of beer again, is the way you manage a complex system is edack error detection and correction. So you have to assume that your system will fail and you have to put a system in place that monitors it and keeps it within bound. Then you have to assume that that system fails and so on and so forth. And it's how complex organisms like ours develop homeostasis. The digital domain is sufficiently complex that we need to start to think about those correction mechanisms.  We haven't got them all right yet.  So you know that that.  You know when when we see a deviance from what we'd like something to be, we have to think. Oh, what sort of institutional mechanism would have fixed that? It might be digital, it might not. But we should fix every every example with a how can I fix this systemically, rather than sticking plasters? You don't run around picking sticking plasters on you. Try and steer the thing, right? | | |
|  |  |
|  |  |
|  | | | | | | |
| **Systems Human Machine Danger** |  | | | | | |
|
|  |  | P11 |  | Yes and yes, and possibly emergent properties.  Which you don't actually see by investigating the individual nodes. | | |
|  |  | P11 |  | It's back to, it's back to that. It's back to that.  Functional top down decomposition. They're coming at it from the bottom up and they're coming up from from an asset based approach, and the clue is in the history historical title of of all of this stuff. But it used to be called network defence. | | |
|  |  | P11 |  | so I'll just return to the point that I was going to make earlier because I was a little bit rude about my safety colleagues thinking that everything is about sort of random failures of pin joints with sheer bolts and things.  I think the problem I have with my security colleagues is that too much is about defending the network and the network attached assets to computer based systems. The software and you can actually have a conversation with.  Then for all forever for a day, and never once did they say. But what does this place actually do? | | |
|  |  |
|  |  | P11 |  | So. So you're you're thinking that actually a lot of the problems are going to come somewhere between all of these things. It's that going to be system wide types of problems rather than, yeah. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 286 of 316 |  |
|  | | | | | | |
|  |  | P14 |  | And of course, as we rely on ever more interconnected back to my point about the Internet of Things. | | |
|  |  | P14 |  | And I mean you, you, this is this critical challenge, critical risk management challenge around systemic failure where you get a knock on effect. One thing fails and isn't very significant, but it has an impact on something which is far more significant and understanding.  The complexity of that.  3 dimensional world.  And all the potential links, feedback loops and everything else is hugely important issue. | | |
|  |  |
|  |  | P18 |  | it maybe it's competency and awareness as well as behaviour, isn't it? Yeah, there's a risk that the technology and the assumptions around the technology can just take it, bring everyone with them. And that questioning attitude and the behaviour around it is insufficient to make sure that it's all being engineered correctly | | |
|  |  | P19 |  | because the source of many problems comes not not just from the technology, but actually more from the people.  Yes, if if you if you get side successful cyber taxes, it's often the case that the someones been engineer.  Human engineer.  Yeah, there may be malicious insiders. | | |
|  |  | P19 |  | I mean, people in, in organizations who perhaps don't have the the the maybe have access rights that they shouldn't.  They they can inadvertently to talk.  Yes, you you can.  It can be subject of of cyber attack and then you know we have and then I'll pay for enough and yes.  So I think that's often the of her faults.  Get injected and so yeah, that's interesting.  So it's not.  It might typically be the big boss or someone who has lots of authority, but well, the this is part of the organizational tree. | | |
|  |  |
|  |  | P19 |  | I suppose people shouldn't really be be given more more access rights than than they need umm.  That, that, that could could be seen as as rather draconian but but these things that we have to be taken into account, yeah. | | |
|  |  | P19 |  | that sort of nightmare scenarios are more to do with terrorism. | | |
|  |  | P19 |  | No, they have to keep providing more, more resources in it and it costs.  Am but the complexity of systems is is I think something that needs studied more so in terms of trends as game changes much more complex systems.  Human human incorporating. Yes, yes.  Human yes, sources of of risk. | | |
|  |  | P5 |  | Yeah, but you can certainly disable physical protection devices, cameras, card readers, things and allow a person to get into steal that stuff. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 287 of 316 |  |
|  | | | | | | |
|  |  | P5 |  | And so again, our our biggest things that we typically do is this sabotage and theft type.  And by the way, the theft part are usually blended attacks because you know cyber can't just mysteriously grab with the bits and bytes and pull material away. | | |
|  |  | P5 |  | Umm but yeah, so that's what we're trying to stop is usually the sabotage.  Bottom line is high consequence events, whatever those may be.  You know, if you're in the pharmaceutical business, you know you don't want an explosion, right?  You know, so you're gonna protect against explosions if you're in the financial districts, you know, obviously the integrity of your data.  You want it to be, you know, full integrity there and not come in the next day and find out you have 0 balance, right or worse a -, 1,000,000 pound thing or something. Right? | | |
|  |  |
|  |  | P8 |  | Human side of things. So when we say human, I say human in three things, right? One the ingenious who design the systems when you are doing it. Do you really understand potential human error from the user point of view are you or are you focusing so much on the hackers? So if you talk about the three human, the engineers who design the systems, the hackers, they're also human by the way we are looking into their psychology. You know they are also human.  Today, the users of the system I'm a user of the system. I have a different psychology. I have different.  These capabilities age, motivation. You know, all these things, right? I don't think any of it really considered much in a sense that when we are really, you know, like an educated, our cybersecurity agents and I just can't see it because every time I talk to them, they are seeing it from their angle. They have one angle. They have one angle. And when I tell them that, how are you really looking into the AB bit and the integrative from the potential risk, the user error point of view is that, look, I secured it from the hackers point of view.  I'm sorry, 90% of the cyber incidents are due to human error, so that keeps map at night. So that research is out there is not looked into is not considered the lack of consideration of human error. The lack of consideration of the issue that come with usability. | | |
|  |  |
|  |  |
|  |  | P8 |  | What I'm trying to say is pretty much of like your ongoing ongoing to try to understand with the with the technology, but it is a bit, it's it's not really catching up like in terms of the technology being developed, some sort of mitigation started being developed. But to really understand the root causes and actually to tailor solutions in my view not really catching up at the moment. | | |
|  |  | P8 |  | So you need to look for the process maintenance process also done by humans. Maintenance systems are already taking care of you know or for example in railways now take caring 6 laptops. The bigs are hurting when they need to download the software. They may not do it because they are in pain. This sort of thing. So I can go on and on and on. It somehow links to humans. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 288 of 316 |  |
|  | | | | | | |
|  |  | P8 |  | Because if you give this to me, if I'm trying to do a task, if I have an urgent task, is it human? I will take a shortcut and I will be jumping at any opportunity to take a shortcut. So if the deficient attack which says I don't have, you've been trying to enter the system for about 15 minutes. If you click on this, I will let you enter quickly. Normally I wouldn't fail for it, but a lot of conditions come together combined with my fullest duration with the urgency of the task I'm trying to.  Say task. Please think of an operator point where is that he could be working in nuclear reactor. He might have a task as well you know.  The goal I'm trying to reach OK once again the usability or the lack of good usability or bad system. I've got bad system.  A design cumbersome system, cumbersome system which will frustrate me. Combined with I have an urgent task or a goal that I need to do in a very quick short period of time.  Three, a reason or an opportunity to shortcut.  This is another human factors, a well known research that the humans take shortcuts whenever they can. You know all the designs. Do you remember all the all the all the payments were going that way but he would take shortcut. It's our human nature, right. This is human factor shortcut and the very sophisticated clever. | | |
|  |  |
|  |  |
|  |  | P8 |  | So the problem is not identified even if it's identified, people are not focusing on it, if it even if they do focus on it, they don't involve people like us.  Human factors people, psychologists, behavioural scientists. We are behaviour scientists that we are understand the nature of the hackers. We understand the nature of users. We understand why someone like me or Someone Like You can fall for any phishing attack because human psychology is not a straightforward have I seen it too complicated? I guess so. So. So, so this what kids market now the laws of things that engineers can learn from us while they are designing their systems, they try to make it more secure. | | |
|  |  |
|  |  | P8 |  | The third one is very important is human to system integration, right? So you integrated the infrastructure with the system perfect. Well, fine. We integrated all the systems to all the systems perfectly fine. OK. But you did it all for the perfect human, which sometimes engineer tend to do,  And the perfect human is, you know, young, able bodied, capable.  And 10 ages no, I'm sorry. The humans come in all shapes and forms. We are not all that intelligent. We are not all that we know. For example, you know, we are not all that young. We are not all not disabled, you know. Like I'm changing. And that might develop like an understanding and dealing with things change like as I get older. 20 years ago I could be faster than I'm not. And in 20 years I will be even less because it's just human nature human nature. | | |
|  |  |
|  |  | P8 |  | I would say one thing that the human factors engineers is we are looking into is a lot of it is integration. This is 3 different type of integration. One is infrastructure to system integration. That is for example you know in an old let's say the truck line or a old rail line. If you put a new brand new shiny train, if you don't integrate it properly it just it doesn't work just because.  So when I say system, please consider in that way system is anything that the humans are interacting with. So in my head a train is a system.  A user interface. It signals a dealing with is a system. A ticket machine that the passenger is dealing with a system. So when I say system, I mean all of it. So integration of infrastructure to any system is where the changes will happen and popping will happen. We are pushing for this to happen so things will be more safer, efficient and effective system to system integration that means.  In a control room or where the drivers or the passengers look, there are six seven different type of systems right. There is one computer here, one CCTV there. One thing there are they.  Integrated. Are they all usable? Are they all intuitive or are they confusing the hell out of human being and increasing their workload? This is why we are coming in. Workload could be for the operator, workload could be passenger workload. If I'm trying to check in and you give me 15 things to integrate with just because you didn't consider. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 289 of 316 |  |
|  | | | | | | |
|  |  | P8 |  | The sort of the people who may be vulnerable to a cyber attack from the personality wise, for example, are more of like an agreeable people. Even there is some research, we say if they're young and female and not agreeable. So a combination of sort of.  They say the human side of things, right. If the humans, whether they're operator or a normal user, is just trying to make some shopping, if their personality.  If, for example, today in live that sometimes you're more tired during the day that the conditions pit magic environmental conditions, you know I am more like an aware of things at 10:00 AM. I'm not so much aware it too too early in the morning if I'm stressed, if I'm rushed so.  The the human factors are anything from personality team to the time of the day-to-day of stressors to their inherent limitations, capabilities, expectations. Quite often we don't look for an attack or we don't expect it. So all these things, if they're combined with.  Umm, I would say systems that did give way for it, which means they are not very usable. So for example if the system is very cumbersome a while ago like can I give an example you're asking for, I don't know 10 digit #5 correct as my memory is already failing me. You give me 10 digit #4 characters, 50 special numbers two AMI am not going to do that. So the system is almost forcing me to make an error. | | |
|  |  |
|  |  |
|  |  | P8 |  | Or the bed systems bed system design. I call it bed system design is unusable systems.  The system is not usable. It is not secure and it's my view, OK, if it's not usable. If it's not secure. If it's not secure, then it's not safe so so so the usability link to safety is not in nice to have, so this is not considered a lot. Other people think that usability of the system is nice to have. It is not. It's at the heart and soul of safety. It's not considered. | | |
|  |  | P8 |  | It's a system problem, but Alice is fully automated, even if it's fully automated. Who designed it to be fully automated in the 1st place, and was it done right so because processes are done by humans, I link it to humans. You see what I mean? So the human fail, but it's not the human failure, it's the process failure. It's the system failing. Yeah, yeah. | | |
|  |  | P8 |  | You mean the users, isn't it? You don't talk about engineers, the users. OK, so, so the training is only one part of the story. So the so the people are not all trained this trip. However, the training is only one part of the story and it may not always be beneficial. The reason being because we get trained on one thing and the thing changes later on or we get trained in one thing.  Forget about it next month. So in terms of sustainability of the training is the problem. So therefore I cannot really provide the training as either A cause or a solution. So the so basically it is a part of the problem, but it is just a part of the problem. People put a lot of emphasis on it, but to be perfect owners, I think the processes are a bit missing in this game. Like if you are talking about, let's say nuclear reactor, different industries and so on, they should be a proper process.  In terms of how to notify like how to notice something went wrong? | | |
|  |  |
|  |  | P8 |  | A lot of mitigating strategies are being developed without really understanding why things are happening. So if you ask me where should we put our effort, I would say not. The question hasn't really answered yet. Everybody's finding a solution. | | |
|  |  | P9 |  | And they do tend to drift as well. That's one of the other things about really complex systems is they tend to drift into positions. And unless you've got a meta system which is forcing them back in again, they will drift into places you don't. So Stafford beer talks about this in his organisational cybernetics, work around control systems and control systems and control systems. The final control system in societal terms, is a revolution.  And if you if your government system deviates too far. | | |
|  |  |
|  |  | P9 |  | We are not managing information risks properly. We're managing information risk by trying to manage data, wrong thing to do.  And until we get that right, we're going to continue to have policies that make life harder and more difficult, and that will have implications for privacy that will have implications, implications for risk, ownership. It'll have implications for liability. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 290 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Technology Life Expectancy** |  | | | | | |
|
|  |  | P11 |  | Well, let me just just tie that point off. What I have said to people over many years now is that there's.  A disparity between the amortisation.  Expectations for a plant. Let's say I'm putting let's take something topical, like a a blast furnace. I'm going to put a blast furnace in in Port Talbot.  It's going to last 50 years.  Therefore, the control system will last 50 years, right? Well, wrong.  Because the nature of the technology on which it is based.  Has an assumed useful lifetime that is incompatible with the things that it's controlling anyway, it's that we can go on discussing it, but it's that fundamental problem that people aren't building in the expectation to either have to upgrade or replace the control systems. They hadn't, at least in the past. I think they're now getting hang of it.  But there's a heck of a lot of it out there already, and it'll still be there in 20 years time. | | |
|  |  |
|  |  |
|  |  | P11 |  | Exactly. Yes. The easiest. The easiest way to do the simple thing is to to bring in a massive operating system.  When I was talking earlier, I wasn't distinguishing between hard between hardware and software particularly, I did mention it a couple of times, but I wasn't. When I was talking about complexity.  I see the boundary between them being quite difficult to distinguish in terms of their contribution to to complexity, because for example the integrated circuit.  May have is it 2 billion transistors and has been has been laid out by a CAD Cam system that was written in C + + 20 years ago.  Or see or something. | | |
|  |  |
|  | | | | | | |
| **Tracking existing attacks and failures** |  | | | | | |
|
|  |  | P10R2 |  | Oh no, this was this was what they I literally put in anonymize. This is this is absolutely not about saying, oh, IBM had a hack on their something system and giving it to the newspapers. This is about some sort of conglomeration 5 big companies have had this amount of problems sort of or or lots of people have seen near misses on that was what they were talking about. | | |
|  |  | P10R2 |  | Yeah. Well, we kind of already have that in the NCSC reports. But legislation to ensure anonymised data sharing of all commercial cyber attacks, that's that's. That's huge. I mean, we're already, I just and I and anyway that all the conversations that I have with with government legislation and I'm talking like civil service as much as you know you know DC are not legislation regulation is not you know it's just not in in scope. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 291 of 316 |  |
|  | | | | | | |
|  |  | P10R2 |  | So yeah, I I in fact, I'm. Yeah. So so I think the mixed economy that we have, so you know the kind of threat reports and things that we already have don't see legislation in this space at all but but the the number the you know the number is is is huge and only going to grow but I don't see it's as a tracking I think is already already in play we we could and possibly should see more more thinking about near misses but again I think NTSC do do really good work around this anyway but yeah I don't I don't see legislation or or kind of data sharing albeit anonymized.  Around around those, particularly in the commercial.  Space, yeah. | | |
|  |  |
|  |  | P10R2 |  | Yeah, I know. I I I, I don't. I don't see that changing radically.  Not least of all, I mean, I just I'm. I'm doing. I'm being chronocentric in the way that I'm often critical of other people doing futures of being. But but looking at extrapolating of, you know, the last kind of 5-10 years.  The around around breaches and you know or or threats in in supply chains and with the work that the NCSC does.  Really, that strategically not doing this kind of thing because they want people to share share information, share data and if they're then broadcasting this, there is a commercial dimension to this. So I I I don't see that as as part of the the kind of future landscape.  As a mitigation. | | |
|  |  |
|  |  | P11R2 |  | Yeah. And that is what you end up with. That is what you end up with in, in organisations like GCHQ. In fact, it's the only organisation you could, but this was the European Union initiative where you've got all sorts of other countries in there, some of whom are actually more sympathetic to some of our opponents. | | |
|  |  | P11R2 |  | I see what you mean. So the fact that so you need a trusted organisation that is trusted to be so cyber secure and so human secure that you know in the sense that nobody's nobody in it could possibly be responsible to another master. Yeah. Which is impossible. Yes, I see that. Yes. | | |
|  |  | P11R2 |  | And then there are attacks against some of that infrastructure.  Who? Who are you going to report that to? Are we going to report that to China?  Are we gonna share with China what we can see? The fact that we can see it and we can't see it?  Who are we? | | |
|  |  | P11R2 |  | So the people who aren't part of this just haven't been invited. | | |
|  |  | P11R2 |  | Indeed, yes, that's that's. And it's an interesting. It is very interesting to hear where the pushback would come from. Yes, yes. | | |
|  |  | P11R2 |  | Alright, that's part of the pushback. Another pushback would be, so let's say we.  Invest in a nuclear power plant with joint funding from France and China. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 292 of 316 |  |
|  | | | | | | |
|  |  | P11R2 |  | Right. So you're right, and you've got you've got two things in there. You've got tracking and then you've got forcing people to share it.  I don't believe you will ever force people to share things.  And I it was a big, big debate about this in the European Union when the NIS Directive was being put together.  I think originally they wanted to put legal obligations on companies.  Release information in a certain way. I have to be careful what what I say, but let's just say that there was some. There was some scepticism that this was actually workable.  There are all sorts of reasons. It isn't very easy to make this work, one of which I won't go through all of it, but one of which is that the very people that you would be reporting to are probably the people who are involved in attacking you. Or rather, it is very hard to keep the people who are attacking you out of the reporting system that you would be legally obliged to participate in. | | |
|  |  |
|  |  | P11R2 |  | Well, I think I think the way you do it is you establish trust between individuals on a on an on the basis of need.  And you create groups and those groups do exist already.  But they're just not declared, and if you aren't part of them, it's because you haven't been invited. | | |
|  |  | P11R2 |  | Yes, because they were not allowed to do this kind of thing. So it was at jeopardy to their jobs that they shared this information. They were not permitted to reveal it to anybody. They were under strict obligations, but they still helped each other out. So in other words, it happened despite the system.  And and it worked well.  But as soon as you formalise it, you end up with a situation where the requirement is that one organisation trusts another organisation that doesn't work. Organisations don't trust each other, people do. So I'm I have a complicated reaction to people who.  Suggest that the answer is that we should all be forced to tell each other when bad things happen. It's naive.  That's my reaction. | | |
|  |  |
|  |  | P11R2 |  | Yes, but it's because they had loyalty to each other. The lawyers absolutely prohibited it. | | |
|  |  | P11R2 |  | In the in this context, so in the context of an international environment and some of these regulations are are sort of transnational, there are some difficulties there. Now. I think what we currently have is something that is far more.  Nationally based and.  I'll tell you now. I'll. I'll tell you one final story.  A long time ago, a friend of mine talked about how the banks work together and he said the IT people, the IT security people of the banks have all moved around and many of them have done each other's jobs and they meet down in a bar, you know, in the in the pubs in London and they help each other. But the lawyers, sorry. | | |
|  |  |
|  |  | P12R2 |  | OK, checking existing failures, legislation systems you're trying on my data. Oh, my God. I hope that that happens. And is it appropriate? Is it appropriate? Yes, of course it is. OK, strongly agree. | | |
|  |  | P14R2 |  | Systems | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 293 of 316 |  |
|  | | | | | | |
|  |  | P14R2 |  | 'Cause I know that is at the moment, I think it's the computer Misnuse Act 1989 or something actually criminalises the activity that security teams need to do in order to understand the threCecilats they're facing. | | |
|  |  | P14R2 |  | There's a here we are the Computer Misuse Act. 1990 is outdated. It criminalises what security teams need to do. | | |
|  |  | P14R2 |  | Yeah. Yeah. So yeah. So legislation is rarely needed to help track existing attacks and failures. | | |
|  |  | P14R2 |  | I think they might even have a website and you'll find her paper and stuff they've done on that. | | |
|  |  | P14R2 |  | I've just been looking at something.  So there's no protection for whistleblowers reporting problems in cybersecurity, no protection of the security industry for legitimate and proportionate security research. | | |
|  |  | P16R2 |  | Digital infrastructure operators this kind of knowledge. So I think this is really a mitigation technique we need to develop. We need to make that knowledge as broadly available as possible to as many people as possible with metrics that they can actually use and they can.  Embed into their own systems to protect them better. | | |
|  |  | P16R2 |  | So we we don't have any.  We don't have a attack or failure monitoring programmes well. The private companies do actually that because they.  Or stepping.  You know, in the shoes of of government and they are selling services where they they sell well they what they call intelligence feeds and all of that because companies need that knowledge. But the government is not really governments are not providing companies or the whole. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 294 of 316 |  |
|  | | | | | | |
|  |  | P20R2 |  | I think that might be legislative overreach. I think there might be some pushback against that, but I think.  You know you can you can compel a whole country to to share everything. I think you know.  That might be over regulation, so especially with our government currently, I don't think that that would be you'd have the you'd have the the Tory right up in arms about that kind of nonsense, but anyway. | | |
|  |  |
|  |  | P20R2 |  | I think you need to find a balanced solution to this, but certainly more sharing is a good thing. But whether you're going to be able to legislate it on that scale, I'm not sure.  Core reasons, | | |
|  |  | P22R2 |  | That, but it's absolutely true., who's trying to do it? What have they included? What haven't they? And it's clear that you can't actually do it, to be honest. But what you can do is you can.  Measure. Instruct in terms of the straight access to a service.  Like you either have a service or you don't and you can get user hours lost.  And that's a really simple mind. You think, and it's something that came out of some easy work and it's published by the NIS as their framework, and they use it to find RGS PS registered data service providers for data breaches. | | |
|  |  |
|  |  | P22R2 |  | But they haven't used it for service outages.  And so it the proposal that we are are putting forward and trying to get acceptance for it. Here's this frame. It talks about these things. When you start thinking about how you might measure these, it starts to get you can get your arms around it because you can measure data breaches. Nis are doing it well. ICO are doing it for.  The whoever they are now, they're in GCMSI think still, but they've major gone to GSITHI do.  But they have suggested in terms of their guidelines that service outages, big service outages ought to be the same sort of reporting structure through the regulator.  Now that's hold that thought. That's good. That's a start.  What the regulators are saying to us when we talk to them is that actually for CNI, you need continuous monitoring of small incidents.  Because of their complex, tightly coupled systems.  That display the characteristics that are described by natural accident theory, and so you need continuous monitoring of small almost failures in order to build up data to anticipate and prevent. | | |
|  |  |
|  |  |
|  |  | P22R2 |  | Yes. And in order to do that, you need the numbers, yes. | | |
|  |  | P22R2 |  | The answer, and I think what we're trying to do with this is articulate the question. | | |
|  |  | P22R2 |  | Because | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 295 of 316 |  |
|  | | | | | | |
|  |  | P22R2 |  | Major failures.  Now it might be interesting talking to the people in the nuclear industry about natural accident theory and how they monitor, because one of the things that I don't know is.  How up to date?  Their monitoring structures are and whether they could be incorporated straight into other parts of critical national infrastructure because they've got nice headings about how to anticipate events and how to monitor events. And but they probably don't probably don't have any.  George Data acquisition stuff because they're probably, you know, several generations behind, but. | | |
|  |  |
|  |  | P22R2 |  | Data acquisition and analysis comes out as a big question. How do you do data acquisition? Well, that's quite easy. Lots of sensors around.  And analysis? Well, that's where IO comes in. | | |
|  |  | P22R2 |  | So there's a there's a picture that emerges, that of what is really needed to get arms around the risks to critical national infrastructure. | | |
|  |  | P22R2 |  | Using the NIS framework as a basis for counting three things for every event. Yes, counting the output for real events. But there's a second thing which is actually rather different and is probably going to be more sensitive, which is you'd you'd also want, particularly with really sensitive things like probably electricity or or nuclear.  You want to know the minor details.  That haven't this time led to a minor outages that haven't this time led to a an event, but that but that could do. | | |
|  |  |
|  |  | P22R2 |  | Exactly. Now to hold that thought, now this requirement came out of the regulator as something they'd like. I don't necessarily think it has to be a regulator, but it is something that the organisation should know about. Now, you did have a point in your definition of C and I that they waited for the regulator before they did generically. So in that it probably is the regulator that has to suggest it.  I've seen other industries that are less heavily regulated are perhaps, you know, the board might take a view of this. | | |
|  |  |
|  |  | P22R2 |  | And it's clear we need risk management. Resilience is all part of, you know, I mean that's OK. We need resilience to get that. We need risk management to get that. We need numbers, we don't have numbers. Let's go back. Yes, yes, yeah, yes. So. So you're not disagreeing with the first two. You're just saying you can't do them yet. | | |
|  |  | P22R2 |  | Like you know, the bonus point payment for employees, you know, most employees will trust that it will come back up and get the right answers eventually. But so it's a question of setting priorities and that's why I thought that the thing you've got #8 should be #1.  That's tracking existing attraction failures. I think that needs to be measuring tracking attraction failures.  And adding to that.  After the sentence, this could drive priorities in investments by suppliers and investment in infrastructure. Supplier is said the software supplies and there's infrastructure suppliers and the IT department in infrastructure suppliers.  The IT DEP.  Need to know what is crucial for their organisation at the moment they don't because there's no data.  On the size and shape of the failures that are happening.  They don't know when something goes down, so they they do an mttr they do an mtbr right. Meantime to infer this Mtbs. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 296 of 316 |  |
|  | | | | | | |
|  |  | P22R2 |  | And they have no idea whether that's a million users without electricity or five.  So there's no impact for that. And so I would have put another point in terms of risk mitigation.  Which is using the NIF and using the NIS framework.  Of lost user.  Damage to Jas.  Damage to health and damage to life and health.  Financial damage.  To set priorities. | | |
|  |  |
|  |  | P22R2 |  | Apart from anything else at the moment we don't have a way of doing that risk assessment really. | | |
|  |  | P22R2 |  | OK. So so we're pushing this up. So they're pushing up the tracking. Why? Because it allows you to do the risk assessment. | | |
|  |  | P23R2 |  | Yeah, it's yeah, this is a big it's still still not solved.  From the deterrence theory approach, right that you know expanded shield, if you can get that tracking.  Shared defence. We still don't have that right. | | |
|  |  | P24R2 |  | prediction and detection, yes.  Systems testing, yes.  Trucking existing attacks and failures.  Follow up and like lessons learned so. | | |
|  |  | P3R2 |  | Exactly. And if you're kind of there, then let's just you know. And if so, if you're immature.  That's the people that you want to try and legislate against and you know, so they're gonna help them.  But if you're already pretty mature, you're probably already doing that sort of thing anyway, so there's a. So there's a, you know what I mean? | | |
|  |  | P3R2 |  | Yeah, but I I, yeah. Again, I don't think with that bad at the moment to be honest. | | |
|  |  | P3R2 |  | No, the NCSC collects this sort of stuff and probably knows a lot more than they tell us. Yes, yes. | | |
|  |  | P3R2 |  | Yeah, the NTSC and and then you know sectorially.  But I mean, at least in in Europe and probably the UK as well, sectorally that you know there are networks for information sharing that already exist. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 297 of 316 |  |
|  | | | | | | |
|  |  | P3R2 |  | That are reasonably mature.  You know, there's isax and sector specific kind of certs and stuff like this.  And I don't think legislation's the thing to sort of force the hand of that becoming more prevalent. | | |
|  |  | P3R2 |  | Two issues there.  I'm not sure legislation is the key. | | |
|  |  | P3R2 |  | 'Cause I I guess it's not a thing that you want to do. You don't want to do it from a just purely compliance point of view. | | |
|  |  | P3R2 |  | So 'cause I think where that kind of sharing goes on at the moment, it's not a compliance driven thing. It's a sort of people understand there's a benefit associated with it.  You know, it's a communities of trust, that sort of.  So that feels to me one aspect of it. And I think if you if you're coming at you, so when when does that sort of thing become useful when you have a the means to do something with that kind of information?  It's a security maturity question, right? But you know, you can throw all your, you know, whatever anonymized data at me until I go blue in the face. But if I don't know how, if I can't do anything with it.  Right. Because I'm in other places, I'm completely behind. Like I don't what my assets are. You know, I'm not doing any monitoring, blah, blah, blah, blah. Then it's a waste of time. | | |
|  |  |
|  |  | P3R2 |  | To to enabling that.  On doing more of that.  I think you sort of have to show the benefit. | | |
|  |  | P5R2 |  | Men quandary on this one.  Because OK, if if if.  My first response is absolutely we should be doing this, however.  Soon as you get legislation and government involved in any of this, they always mess it up.  And I don't know how they can anonymize and protect people's data, so I'll tell you a quick little story at the IAEA. I've been in several meetings years ago where they wanted to maintain a database for everybody around the world for their nuclear facilities of incidents.  Nobody trusted the AIAEA that they weren't gonna be breached and their data of an embarrassing incident would get out everywhere, right? So people are reluctant.  Talk about.  There are issues on cyberattacks and software failures, so I don't. I'm not this. | | |
|  |  |
|  |  | P5R2 |  | You know what? I'll maybe maybe a little bit it should I agree with that. I just don't know if it's gonna happen. | | |
|  |  | P7R2 |  | I'll I'll put some would agree here because on the on the tracking existing attacks and failures. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 298 of 316 |  |
|  | | | | | | |
|  |  | P7R2 |  | In the sense that on one hand it's it's correct. I mean the statement is correct on. On the other hand, there's only so much you can share without exposing the the existing infrastructures further. So there is there's a tension there. | | |
|  |  | P9R2 |  | And they've tried to set them up in other sectors, but it takes a long time to get to that trust. Now. The banks actually have had to learn to trust each other over the years on all sorts of things, including Libor rigging and other things. So not always for good reasons. So the difference there, I think, is the do you want to establish sharing of risk information to manage risks or do you want to publicly share all of the risks? | | |
|  |  | P9R2 |  | Does that have any name or something one can reference? | | |
|  |  | P9R2 |  | And share, but actually.  Experience of so there's a there's a cybersecurity information exchange.  Model that works across industry for this already.  And it works.  Behind the scenes, rather than in public, but it works because it's behind the scenes. So amazingly, the banks, for instance, that meet with NCSC on a regular basis in a closed room, and they talk about who's hacking them, how they're hacking them, how they're getting in, they take notes, they go and fix it. None of the banks take any of that information and use it for commercial advantage. They earn the right to be in the room by earning that trust and by being in the room, they get to go and fix their problems. So they know that they're working in that room for the sector as a whole and not for their individual banks. It's brilliant. Mechanism works really well. | | |
|  |  |
|  |  | P9R2 |  | Yeah, I think it's cool. I think it's csex. I think it's a cybersecurity information exchange. | | |
|  |  | P9R2 |  | With the intention of providing accountability instinctively, I'm a fan of that. But I think there are real problems in getting there from where we are today.  Because of the way that the public would respond to what they learn about the resilience of the systems that are in front of them. | | |
|  |  | P9R2 |  | I think I I am a strong proponent of radical transparency when it comes to these systems. I think what undermine my ability to go yes do this thing is you can't do it in isolation of fixing the entire commercial model around these things. So this is one of those areas in which companies would say we'll all do it if you regulate. | | |
|  |  | P9R2 |  | 90% of the work you do for the next 10 years will not be productive. It'll be dealing with the noise and you, you you might miss the value of saying actually what I really needed was this this to happen so.  I like it.  I have that caveat about her. | | |
|  |  | P9R2 |  | OK, so I think it's a really serious idea. It's got to be given serious thought, but the serious thought includes don't rush into this panic slowly. Let's take the right steps to get there, because if you shift from a position of blissful ignorance to everybody knows everything. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 299 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Tracking Existing Attacks and Failures** |  | | | | | |
|
|  |  | P12 |  | a privacy legislation could actually do more to force disclosure about critical infrastructure dependencies and and. And all of these kinds of different dependencies. So yeah, see. So again, I actually don't know how that works constitutionally in the US, but I know we have a defence production act that would provide.  Some tools to I think.  You know, force these kinds of disclosures. So some chaining of privacy legislation with maybe a defence production Act, you'll disclosure requirement actually could be really helpful and and I think that that would be a much more robust because privacy means a lot of different things. Obviously it's very contextual. But but the really the boundary between privacy and security is is pretty porous. So I think using this as an excuse to to to force more of these disclosures and like you know where is the data stored like a data locality kind of you know EU has this kind of data locality thing as well. | | |
|  |  |
|  |  |
|  |  | P22 |  | And so that's another of the reasons why we pulled back to say, impact measure. What's important, measure the failures, find out how to fix those. Yeah. Look to look at real life, not a theoretical approach. | | |
|  |  | P22 |  | so unless the regulators change their stance, I can't see, you know, I mean, I'm in the Thames Water area. Yeah. I can't see Thames Water changing its policy unless it is quite heavily pushed to do so.  Because you know so much of the industry, the that supplies this infrastructure is not owned in the UK and so it's only really at the point of use that you can regulate.  And that has to be by regulation in terms of.  Measuring, you know, the impact of brakes, so going back to the Nat structure, you know it's it's crude, but it's a structure, it's it's availability and we're you know and it introduces this concept of user hours and a concept of lost user hours is a really useful change in focus for the IT guys. | | |
|  |  |
|  |  | P22 |  | there is no data.  There is no data on either the frequency or cost of failures.  There is a framework.  The Nats framework you've come across that, yeah.  And government could use it that they've chosen not to, but it's not. Got sort of onto their critical list. | | |
|  |  | P22 |  | So there is a framework for actually narrowing failures. Now. If you talk to xxx, she'll say that's such a crude thing. She'll want all sorts of other things, but actually it's a start. If you can persuade governments to.  On it and even start with, not just trying to influence regulations to influence infrastructure companies, etc. But if government started to publish their own data, that would provide a role model and it would allow people not to feel guilty about software. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 300 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Training in Digitisation** |  | | | | | |
|
|  |  | P19 |  | so software is it's not magic, it's it's it's it's, it's logical and people we need to be not frightened of myself, but they need to be trained to know more about it.  So you see, this is an education.  Yeah, absolutely. Yeah.  Yeah, putting in these traditional industries, yes, like process control and utilities that need to be more people and and they're doing this anyway. | | |
|  |  | P19 |  | People who know about software, people who know about Sandra types.  Yes, Sandra defects.  They the the.  Yeah, of course.  That's very important.  So this is training skills and awareness. | | |
|  | | | | | | |
| **Training in the Management of Innovation** |  | | | | | |
|
|  |  | P18 |  | I've been doing some work with with IAA and International Atomic Energy Authority around competency and innovation.  And the model that we've come up with is for any application of stuff new.  You need three people.  You need a person who's competent in the technology.  You need a person whose competence in the application of that technology. So. | | |
|  |  | P18 |  | More you know, experts in you know, whatever you wanted to apply it to and the third person you need is someone who's competent in the.  Process of implementing innovation.  So being that that kind of.  The precautionary principle, you know, knowing, knowing, kind of how you go through the process of developing technology readiness levels and you know the ways of mitigating risk because of that. And I think I think that stacks up an awful lot that between those 3.  Skill sets you can end up with effective deployments of some stuff new, but take any one of those three skill sets away. Then you're leaving yourself vulnerable to either.  Not going down a due process or not having the right level of information on the application or not having the right level of information on the technology itself. So I think that's that's a helpful model to think about.  Those behaviours and kind of competencies around the deployment of innovation. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 301 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Training Staff about AI Threats** |  | | | | | |
|
|  |  | P16 |  | So that's the I think probably the high level answer and the low level is try to train.  Retrain everyone to with working within those organisations, not cyber security specialists.  The all the employees to help them.  Understand the new AI threats. So those I was just reading before Oracle the the new report by the.  Your National cybersecurity centre.  Where on AI threat and who's going to make the most use of it. And they were explaining that we're going to have to train people to understand that now any e-mail that you receive from anyone can be coming from an AI and not from a human.  Still be very, very persuasive and be be perfectly. | | |
|  |  |
|  |  | P16 |  | So learn teaching people that you know.  That's life, the new life. And there was a report a few years back in the US that used analogy I really like.  It's surviving on the poisoned fruit, so you're surviving. You're learning to survive.  Eating really crappy stuff and you're making yourself anti fragile.  So you know that your systems are very fragile. There is not much you can do about it and you learn to live with that state of uncertainty and stress, and you carry on. | | |
|  |  |
|  |  | P16 |  | Exactly an exact reflection of a of a authentic e-mail. So training people to not trust the first site, everything they see and they get in their inbox and and make decisions accordingly. So I think we're also going to have to in terms of human interactions with machines that we're going to have to redefine our understanding of.  Trustworthiness and.  Protocols for people to make important decisions.  And to validate and authenticate authenticate.  The content of information, so I think it's gonna be an interesting few years to kind of redesign all of that and to retrain a lot of people. But it's gonna be an evolution, not a revolution, I think because now AI becoming so embedded into everything | | |
|  |  |
|  | | | | | | |
| **Trust** |  | | | | | |
|
|  |  | P11 |  | How do we know that this is going to wait?  How do we know that that digital twin is integrity is intact? | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 302 of 316 |  |
|  | | | | | | |
|  |  | P11 |  | Since we're on digital twins, let me just make an observation in passing, there's.  Lyapunov there's there's some mathematics by Lyapunov. I'm told I'm not a mathematician.  Like a Lyapunov, I think coefficient which one can apply to to modelling like a digital twin which essentially.  So this is how it's explained to me by a mathematician. If I have billiard balls, I have some billiard balls. No, I want to calculate where the third bounce will go. Then it depends crucially on the angle of departure and the radius of the billiard ball. And there comes a point where I can't measure them sufficiently accurately such that I'm at a point of N it's just chaotic.  Well, you can regard that as being a good model for, for example, the weather forecasting system.  And the digital twin that's going to be running the SMR, that'll be just down the road from you, you know. | | |
|  |  |
|  |  |
|  |  | P11 |  | Environments like Smrs will only be economically viable if they use technology that isn't currently regarded as being appropriate to those kinds of.  Safety critical environments, so you can't always get the sensors you want and the places you want. You can't always have individual wires going to every last sensor because there isn't the space and they're sealed for life.  So you end up having to do in make inferences to parameters rather than.  Bring them directly. May not be able to measure a particular pressure in a particular place. You may have to make some form of inference.  Using and here it comes using a digital twin.  And and so I see quite a lot now that's that's a sort of development beyond what I referred to earlier, which is that prognostication prognostics and diagnostics there we are.  The prognostics and diagnostics are effectively done, even if they may not be advertised as such against a digital twin.  And I think the question is. | | |
|  |  |
|  |  |
|  |  | P11 |  | Right. So so this is something you can you can have all the digital twins in the world etcetera, etcetera. First of all, they cannot reflect exactly what's happening. And secondly, there's a measure of indeterminism about what's going to happen anyway, is that. Is that what you're after? Yeah. | | |
|  |  | P11 |  | And and bring it back to that digital twin for the for the weather forecast.  How do I determine the limits of my confidence in the outputs of the machine learning algorithm? | | |
|  |  | P12 |  | , when I look at AII really see this is almost like the way I would look at like a compiler where like we had assembly, right. And then there's this compiler that's interposed between you and the actual assembly code.  And as you work your way up that stock, you know with Python I don't even know what's happening at the C++ binary layer, let alone what's happening assembly. And now I think like AI and generative AI in particular has really interposed at a level above where, you know, I know people who are using, you know, llms to generate Python. And that's just another layer of interposition. And I think that as AI interposes more and more in that stack, the more it becomes difficult to discern what's actually happening. And I think to this question, yeah, that does potentially make it harder to discern whether something was.  Misconfiguration or yeah, an an attack. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 303 of 316 |  |
|  | | | | | | |
|  |  | P14 |  | What's really interesting, especially talking about the cybersecurity behaviours piece, is how people will say to me, of course, AI machine learning might be able to help, but also there are real concerns.  First and foremost, one that you'll get more than most is just the trust question. So, so much AI and machine learning goes on inside the black box.  For the ordinary lay user customer client stakeholder.  Are they going to buy this if they can't have it spelt out in sufficient detail to make them feel reassured, this is going to deliver a robust and reliable service that's explicable and there's, you know.  In a separate life, I I I found it a early stage company back in 2014 which was using machine learning to help video analytics and one of the issues there was. | | |
|  |  |
|  |  | P14 |  | In particular, to help law enforcement, and you know, if you.  Bringing someone to court based on the video analytics.  The judge might want, and the jury might want to hear an expert stand up and explain.  How they can be confident in?  That capability.  And frankly, what I you could do your best to explain it, but frankly one of the most.  Reliable options would be to say the human has been in the loop. You need to question the human who reached a judgement based on the data that he or she was presented with, and to then explain the steps they took so you know the person in this video looks very similar to me to be the person who appeared out of the bank with a bag of swag on their back.  I was able to track that person to a car. | | |
|  |  |
|  |  | P14 |  | Us to an address which took us to an occupant who had the same appearance as that person, and when we opened the cupboard we found the bag of swag and therefore when you join, that's that, that that's actually dealing with human judgement rather than what the hell it is that the machine learning algorithms are doing. But when you're dealing with how cybersecurity is going to be delivered by artificial intelligence.  Particularly if.  And this is another of the concerns being raised by the experts I speak to.  And then corrupt the learning data. So actually the machine's giving the wrong information. | | |
|  |  |
|  |  | P14 |  | There's going to be a lot of suspicion and anxiety and distrust around AI and ML, and so yes, it could do amazing things. We can demonstrate it doing amazing things, but there's going to be that trust concern. And I know there's a big.  Ukri programme, I think it's 30 million gone into it around trust and AI, which people are worrying about. So that's on the.  That. That's the sort of that's the some of the concerns around AI and ML. | | |
|  |  | P15 |  | Yes, it was Liverpool, but I'm just trying to think of the stadium anyway.  So they had massive issues in that with with the police watching CCTV and saying people were looking angry and aggressive and that's why that's why they took some of the decisions that they took. They took many decisions on that day.  But similarly you could look at that and if an AI system has got programmed in to be able to recognise people's facial expressions but it reads them wrong, then it could lead you to make similar bad decisions. And so it depends on the algorithms and processes and things that are going into doing. If if we are basically substituting human human like interpretation of data with with a mechan like an automated system.  Somebody has to have built that and has to have built in what those things then mean and how to interpret them.  And that then brings into it a lot of its own issues. I think it also kind of it does also have like clear benefits around sort of security management for CNI sites where they'll be very vulnerable sites that will be wanted to will be wanting to protect. So there should be benefits and opportunities around that kind of thing as well. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 304 of 316 |  |
|  | | | | | | |
|  |  | P15 |  | Yes. Yeah. And anything I would suggest, anything where you've got a huge amount of infrastructure which needs to have surveillance on it. And I don't know around nuclear sites, if you don't have exonomy, you've only got X number of cameras and X number of.  CNC the civil nuclear Constabulary. They can only be in certain places at certain times. Therefore, like how well see you. Are you managing the the security?  You know, security awareness.  And situational awareness around risks that are physically present at the time and also virtually present and things like that. So.  I think again there are opportunities, but again there are opportunities and threats for those systems to be infiltrated. | | |
|  |  |
|  |  | P15 |  | Like AI in crowd situations and reading people's expressions like one of the one of the major findings from.  The football crush, the football stadium crush where 99 people died. | | |
|  |  | P16 |  | Exactly. Yeah. I mean, I just like, I mean, you read probably like everyone else, this poor fellow, poor chap in Hong Kong that was lured. I don't if you've seen it, it was lured into a zoom call with six other people from his company. He was working in Hong Kong. I mean, he's working in Hong Kong and his bosses were in the UK. So he was summoned to a zoom call with six people requesting him to wire $25 million to an accounting in the UK.  And actually, none of those people were real. They were all AIS, and he was actually.  Manipulated into wiring this massive.  Amount of money, but only by AII mean. No one ever so. So yeah, it's going to be really.  Complicated and tough to to verify the authenticity of someone now more and more. | | |
|  |  |
|  |  | P16 |  | Complexity.  And very often by companies that come from very different sectors, from very different understanding of what security is about. And it's very.  Very sophisticated companies because of the levels of investment required and they're very hard for the customers to really know what's happening in those data centres and to really have a guarantee of their so. So I think really cloud computing would would be.  For me, the the really critical.  Component of of of those? Yeah, as a trend, it's something that it is really super important.  E-mail problem, yeah. | | |
|  |  |
|  |  | P16 |  | Cloud computing technologies, upon which those critical infrastructures more tend to rely more and more. So what we found is that the banks are very worried, for example about their.  Ability to guarantee that they will keep on being able to trade even during a crisis, because now they don't control. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 305 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | Computing systems directly anymore, but they rely on 3rd party providers.  Of which they know very little about, so it's easy for a bank to ask to see what's happening in the systems of their partner financial traders, because everyone has to abide by the same type of regulation, and so they trust each other. They know they have to operate, but then it's impossible to ask a financial partner institution to have access to their Microsoft.  Or IBM or Amazon cloud.  Services because those companies are much bigger and they say no, no, no, we just provide a service to you. Trust us. You know, we have thousands of engineers, so it's creating.  Lack of understanding of the the reliability and so the cloud computing. And now I think in the I think in the in the US the the the financial sector regulators are now asking submitting the cloud computing companies that service the financial sector.  To some high levels of oversight as well.  Saying that, if you want to enter this business with a financial.  Institutions, you're going to be part of the packet you're becoming part of the package now, so we're going to have to ensure that you deliver certain levels of services according to certain requirements. I think that the cloud computing, because it's introducing another layer of. | | |
|  |  |
|  |  |
|  |  | P16 |  | Yeah, negotiate. I mean, you use the term negotiating something. You know, it's the the comments, you know, when you when you leave under a a comments system you know we you have to jointly agree with all the other users of the comments that you're not going to over exploit you're going to be and I think this is the kind same kind of.  Configuration where we need to be able to discuss and then to agree and then if we can't agree together, someone has gonna step in, has gonna to have to step in and probably the state and to say no. Now if you can't agree it's it's better if you agree together without enforcement or without and you coercion because it's very often introducing it's on emergent effects that are very often and desirable as well. But if you can't agree for a reason or another then I'll step in but.  Let's try to have a joint.  Discussion or negotiation among reasonable people or stakeholders to ensure that we understand how this interconnectedness is impacting everyone and how we can address it. | | |
|  |  |
|  |  |
|  |  | P16 |  | No. OK. So but yeah, but the legal sector, it's very interesting sector because it's not very tech savvy in the sense that usually.  Legal professionals. They tend to stick very much to tradition and to, but it's it's surprising how critical they are actually to the operations of the critical infrastructure sectors, because any company doing a merger and acquisition of another company has to.  Go through a a a a legal service provider that has access to their most important secrets. Their most important financial statements, and the legal sector, so holds the secret because of the cleaned you know the the the the attorney-client privilege and all of that. So they hold secrets.  The most important secrets of the biggest companies in the world, not not being very sophisticated at technology and keeping.  Under wrap, like the police or intelligence community. And so the the attackers are very knowledgeable of that and and and the target. And I know I know I speak of experience because I've acted as an expert witness in a number of cases that were never, never went to court because no one wants to hear about that or to air that kind of weaknesses but.  Those are cases of.  Billions of dollars in in, in fraud and secrets being stolen on the massive scale. So. | | |
|  |  |
|  |  |
|  |  | P16 |  | Yeah. So yeah, so there's a, there's a. There's a reason why this is going to may well get worse. And it could even be dealt with by human negotiation, you know, iPhone you up and say by the way, you do realise that you are, you know, you're going to, you're going to make us both look bad. But by doing this, but we've got to know to do that. Yes. Yeah. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 306 of 316 |  |
|  | | | | | | |
|  |  | P16 |  | Yes, yes. And we so we we need a even to be able to to know who to phone you. You need maybe to have like.  A A platform of trust from which we can communicate to each other. What what I am doing to you without necessarily kind of wanting to attack you. But what my decisions are doing to you and try to solve it together. So we need to develop.  For us, where we can discuss this and we can try to fix it together.  So that the overall ecosystem stays healthy. | | |
|  |  |
|  |  | P18 |  | Is that all the way through the life cycle? So designers?  Implement a implementers operators and you know people modifying it. You know it needs all of those people to have the right mindset. | | |
|  |  | P18 |  | Yeah. Yeah, because it it's got, it's got an ability it it works very well in three-dimensional space. So if you imagine supply and demand as being a geographically distribute distributed thing then rather than a conventional safety, a conventional computer system will will try and map the impact of each of those things. Each of those nodes, if you like, of energy production, a quantum computer would do that in one clock cycle.  And so because it's because each of the positions on that map can be represented by a vector. | | |
|  |  |
|  |  | P18 |  | OK, so before we go on to that, that's that's sort of basic level of increased digitization, but we've also got things which exacerbated further. So going back to the previous question, there's also other things that exacerbate those issues. So things like artificial intelligence, where we where it's it's very difficult to understand what AI is going to be doing, you know, and how it does it.  And the increased.  Reliance on things like that for people to make decision making and the it's susceptibility to bias if it's not done correctly. So that's another example.  Then I don't know Internet of Things, that interconnectedness of the digital arena means that it's becomes easier for faults for Miss.  Miss operation of your faults within the system to propagate across multiple systems and you get multiple system failure as a consequence of that. So it's the interconnectedness that comes with digital as well, which also causes causes a risk. | | |
|  |  |
|  |  | P18 |  | Can you? So you can try and put traps in into that but but being being aware of that and designing that in. So making sure that whatever approach you take.  To the deployment of these new techniques.  Is built on the precautionary principle where which says that if there's uncertainty associated with what you want to do, then you should put more protection around doing that until you've got the confidence that you've reduced the uncertainty to an extent that you believe.  You know, it's always gonna be correct and you know, and you know, to so many, you know, you know, the reliability of it is X and then you can be more, more proportionate about what you're doing. So. So I think that precautionary principle is really important with with new innovations.  So yeah, my I think it's a behavioural thing. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 307 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | So we're nuclear, I guess the the consequence of that is that we in nuclear, we put a lot of emphasis on lessons learned.  If it's, if you're. If you're unable to detect the reasons why something has failed, then it's very difficult to do. You know the lessons learned and you know that the more complex the technology, I think the less able you will be able to understand why why it's failed. So why AI is given a reason, an answer out. And for instance, which is, you know, is obviously going to happen.  Yeah. So it's it and there's no way of doing that in many cases, you know certainly for kind of.  Generic models then?  Yeah, it's kind of that, that I don't know whether this is helpful, but that that.  It suggests that you need to have that corroboration approach. You know the AI is saying a how are we going to corroborate that and that that doesn't go a, A is not magic. It still needs that corroboration that we've always done. You know, if something's important, you don't just take one piece of evidence and say, look, it says there that it's important and then accept that there seems to be a kind of again it goes to mindset with people.  No, it's AI that could it, so it must be true, you know? Yeah. | | |
|  |  |
|  |  |
|  |  | P18 |  | There's a there's a tendency, I think, for people to be trusting of, of new technology, overly trusting of new technology.  And again, take AI. You know, we've maybe sceptical of it at the moment, but it does do some magnificent things really, really impressive things.  Over time, what does our perception of it?  How does it shift? How reliant do we become on it?  And therefore, if there's errors in that.  Our scepticism.  Maybe reduced and we end up accepting things that are wrong, so I think there's an awful lot around human behaviour in in these these things about.  And you know, and the human behaviour. | | |
|  |  |
|  |  | P18 |  | Oh, what's the word I'm looking for? Contour your profile, then. It's very good at optimising the the flow of whatever from A to B. | | |
|  |  | P18 |  | Then at 1 sample it can do across a whole lot.  And it so it becomes a lot more powerful, a lot more insightful. So it's very good at at kind of trying to solve problems where I imagine it like a map, a quantum computer can draw the valleys and the peaks.  So if it's want to find the the path of least resistance from point X to point Y. If you can represent that into some sort of. | | |
|  |  | P18 |  | Yeah. Suppose I suppose knowing maybe it maybe it's competency and awareness as well as behaviour, isn't it? Yeah, there's a risk that the technology and the assumptions around the technology can just take it, bring everyone with them. And that questioning attitude and the behaviour around it is insufficient to make sure that it's all being engineered correctly. So maybe it is Quant, maybe it's twofold.  Is competency.  And behaviours.  I've been doing some work with with IAA and International Atomic Energy Authority around competency and innovation.  And the model that we've come up with is for any application of stuff new.  You need three people.  You need a person who's competent in the technology.  You need a person whose competence in the application of that technology. So. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 308 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Unexplainable or Unpredictable AI and Systems** |  | | | | | |
|
|  |  | P14 |  | What's really interesting, especially talking about the cybersecurity behaviours piece, is how people will say to me, of course, AI machine learning might be able to help, but also there are real concerns.  First and foremost, one that you'll get more than most is just the trust question. So, so much AI and machine learning goes on inside the black box.  For the ordinary lay user customer client stakeholder.  Are they going to buy this if they can't have it spelt out in sufficient detail to make them feel reassured, this is going to deliver a robust and reliable service that's explicable | | |
|  |  |
|  |  | P15 |  | AI and those opportunities are.  They are inherently unknown because we don't know what we're going to do with them and if you don't know what you're going to do with them, you can't know what that then would mean. Actually, if you did implement that in a very benign way, that itself might introduce additional risks and and hazards that we can't anticipate yet.  And we also can't necessarily anticipate even the people who are intentionally planning and designing how they want them to work or want them to do things, how people then interact with them and would engage with them and start using them when they're out there doing their own thing and aren't sort of being heavily controlled. | | |
|  |  |
|  |  | P15 |  | But similarly you could look at that and if an AI system has got programmed in to be able to recognise people's facial expressions but it reads them wrong, then it could lead you to make similar bad decisions. And so it depends on the algorithms and processes and things that are going into doing. If if we are basically substituting human human like interpretation of data with with a mechan like an automated system.  Somebody has to have built that and has to have built in what those things then mean and how to interpret them.  And that then brings into it a lot of its own issues. | | |
|  |  |
|  |  | P15 |  | AI could be will certainly be useful in terms of.  Being able to summarise huge amounts of data potentially.  That in in a short amount of time. But with that comes a huge amount of issues around how it's doing that summary and what it what it considers important, how it's categorising things and things like that. | | |
|  |  | P18 |  | So, so the whole opaqueness of it is itself a big problem. Yes. Yeah.  And so that so that, as it were makes.  Your job if you're working with the regulator.  Much more difficult. | | |
|  |  | P18 |  | Well, it becomes difficult in engineering terms.  To design systems that you you're you've now eradicately robust.  The systems themselves.  Difficult to go to engineer. It's becomes difficult to.  Get confidence in diversity arguments. You know that this system is independent from another system. | | |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 309 of 316 |  |
|  | | | | | | |
|  |  | P18 |  | . So we like things like.  You know AI so difficult because it's complex, you know, at the end of the day, it's only doing statistics, but but you know it's it's they're very difficult to understand what it's doing because of the complexity of how it does it and the lack of understanding you can get from from that. | | |
|  |  | P18 |  | we in nuclear, we put a lot of emphasis on lessons learned.  If it's, if you're. If you're unable to detect the reasons why something has failed, then it's very difficult to do. You know the lessons learned and you know that the more complex the technology, I think the less able you will be able to understand why why it's failed. | | |
|  |  | P19 |  | having programmable systems put in the middle of them.  On on some of them, they end up.  You using Tonkin and machine learning systems?  I don't like using the word.  Terry I but but but some kind of.  Trained systems data process which are quite quite complicated these systems themselves.  I think the introduced more vulnerabilities than than you might imagine, so it's even more important to think about resilience by design. | | |
|  |  |
|  |  | P19 |  | So computer networks are. | | |
|  |  | P20 |  | And particularly the idea that some people have commented on recently about irresponsible AI development processes, the idea that a catastrophe might be.  Something that could occur perhaps more easily in countries which aren't as transparent about their development processes. | | |
|  |  | P20 |  | So you have those sorts of arguments that are framed in geopolitical terms, and they're about the emergence of, you know.  Sort of arms race dynamics, if you like, around AI software. | | |
|  |  | P20 |  | You know, this idea of sort of rush to release of software, particularly AI platforms, because you want to get ahead of other commercial operators, but also other countries. So you have, you know in my view open AI releasing ChatGPT in a in a way and form that I don't think was entirely responsible where there were numerous vulnerabilities which were observed only after it was released.  And I think you know the this rush to release this idea of, OK, well, we won't. We won't do sort of all that much in the way of proper security testing or risk assessment of the software will just get it out into the into the world and let you know Crowdsource that and and let others figure out what the vulnerabilities are. I don't think that this is a particularly responsible.  Process for software development in the context of AI technologies, and I think it's historically been the same for cyber. We're caught between wanting convenience and wanting ease of use, but but not having very secure products. So I think this has been a feature of the political economy. If you like, of of cybersecurity.  So I think that there's some concerns about software development and how the the the regulation is put in place around.  Commercial competition over new products, which might create risks, including for national infrastructure and then layer on top of the commercial competition. You've got the geopolitical competition where producers of software are saying.  Don't regulate us because if you do, China will beat us to general AI. | | |
|  |  |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 310 of 316 |  |
|  | | | | | | |
|  | | | | | | |
| **Virtualisation** |  | | | | | |
|
|  |  | P11 |  | No, I think what will actually happen is that there will be a a fad for virtualization.  In the same in the same way, but different in that middleware.  Allowed all of the cobalt systems to remain in in stasis because they were understood and proven there'll be something about somehow managing to capture the existing control systems and virtualise them. | | |
|  | | | | | | |
| **Vulnerabilities** |  | | | | | |
|
|  |  | P18 |  | Not kind of the availability of any other. Yep, skills or hardware or anything like that. It's it's it's electricity limited.  Use of digital things is.  Is kind of exponential, you know.  The kind of quantity of data grows exponentially depending on on use then and that limits soon happens, so you know there are. There are people out there looking at the feasibility of using things like nuclear as a green energy source.  That's specifically developed for data centres.  How feasible of that is? I don't know. But you know that's that's an example of the steps that some people are going to to try and, you know, accommodate that growth of data. | | |
|  |  |
|  |  | P18 |  | More | | |
|  |  | P18 |  | I've been doing some work with with IAA and International Atomic Energy Authority around competency and innovation.  And the model that we've come up with is for any application of stuff new.  You need three people.  You need a person who's competent in the technology.  You need a person whose competence in the application of that technology. So. | | |
|  |  | P18 |  | Yep, and. And you know what's the what's the results of that limit?  Does that mean that somehow you know a national infrastructure that's based on data, or is, you know, is underpinned by data and the availability of data to make it to help it manage, you know, if if you've suddenly put a cap on that data, what's the implication for for the national critical national infrastructure? You know, does that, does that introduce new vulnerabilities? Does it make it become more flaky?  All those sort of things. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 311 of 316 |  |
|  | | | | | | |
|  |  | P19 |  | So so we get a chance.  The edge, the increased need for preparation, yes, yes. | | |
|  |  | P19 |  | And that the more the more computing, frankly that goes into the systems.  The more vulnerabilities potentially get introduced, yes, yes. | | |
|  |  | P20 |  | Yeah. Well, I think, I mean what, one of the things that.  I'm concerned about in terms of software development is.  You know, this idea of sort of rush to release of software, particularly AI platforms, because you want to get ahead of other commercial operators, but also other countries. So you have, you know in my view open AI releasing ChatGPT in a in a way and form that I don't think was entirely responsible where there were numerous vulnerabilities which were observed only after it was released.  And I think you know the this rush to release this idea of, OK, well, we won't. We won't do sort of all that much in the way of proper security testing or risk assessment of the software will just get it out into the into the world and let you know Crowdsource that and and let others figure out what the vulnerabilities are. I don't think that this is a particularly responsible.  Process for software development in the context of AI technologies, and I think it's historically been the same for cyber. We're caught between wanting convenience and wanting ease of use, but but not having very secure products. So I think this has been a feature of the political economy. If you like, of of cybersecurity.  So I think that there's some concerns about software development and how the the the regulation is put in place around.  Commercial competition over new products, which might create risks, including for national infrastructure and then layer on top of the commercial competition. You've got the geopolitical competition where producers of software are saying.  Don't regulate us because if you do, China will beat us to general AI. | | |
|  |  |
|  |  |
|  |  |
|  |  | P20 |  | Well, so, So what? You're So what you're saying. Then if I understand is you don't see secure by design really working you you see.  Lots continued ransomware of various sorts and presumably improving in technology AI of all sorts you see.  Worsening political situation leading to.  Being used as a justification for arms race and for for bad basically bad software development, you know, seems bad justification to me, but but then yeah, yeah, that's what you're saying. | | |
|  |  |
|  |  | P20 |  | And more practically, we don't have electronic voting here, but we've had scandals about cyber interference with voting systems in America, which have caused a lot of political controversy.  So that's that's a big concern. I think at the moment and it might not be as you know, spectacular or as attention grabbing as a cyber attack against a nuclear facility.  But it's more the slow societal death. By 1000, cuts type of effect of these sorts of operations, which I find a bit more concerning.  I'm I guess. | | |
|  |  |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 312 of 316 |  |
|  | | | | | | |
|  |  | P20 |  | So you have those sorts of arguments that are framed in geopolitical terms, and they're about the emergence of, you know.  Sort of arms race dynamics, if you like, around AI software.  In terms of.  Software development for critical infrastructure. I don't know a huge amount about it, but historically it appears to be riddled with vulnerabilities and weaknesses in terms of if you look at the state of secure software in those sectors.  Not a lot of protection around lots of industrial control systems. Wanna cry virus spreading globally affecting the NHS, systems that are still running Windows XP.  Legacy software not being able to update it being used globally, which of course creates a whole new, you know, levels of vulnerability.  Yeah, I mean, I I just think it's a, it's a market which.  Is pretty pretty weak still in terms of security, I I I attempt during the pandemic they had the Aspen Cybersecurity Summit, which is one of these big American events. And Alex Stamos was there, who I'm sure you're you're aware of. And he he said something which stuck in my mind, which was that. | | |
|  |  |
|  |  |
|  |  | P20 |  | Bug bounties. Yeah, that they're sort of market market of, you know, will release this software which has lots of flaws in it. You find it for us and we'll pay, pay you for it. I just think it's it's it's quite bizarre really.  It's and and you know this whole the growth of this penetration testing industry for both software and hardware, you know, OK, we'll we'll build the digital network, we know it's not secure, but then we'll hire people come in to to come and test it for us.  You know, it seems to be security after the fact, doesn't it? | | |
|  |  |
|  |  | P20 |  | And you know, obviously you have this software secured by design narrative around software and and and hardware as well.  But you know I'm. I guess I'm a bit sceptical about the extent to which that will change behaviour or people, you know, people will can be or companies can be incentivised to make their products secure by design. It appears to be a, you know, an initiative or a policy direction which.  Is set against some pretty big prevailing headwinds.  Because of the basic economics, I don't know whether I answered your question at all there, Charles, but those are my random thoughts on software. | | |
|  |  |
|  |  | P20 |  | Chinese hackers are very good and US software is incredibly weak and I think that summed it up to me, you know the.  Ability for people to hack into even the latest iterations of software platforms produced by the top tech companies in America. You know, they're they're pretty vulnerable. It's pretty easy to to, you know, gaolbreak the software to find vulnerabilities and flaws in it.  I think this whole you know model of bounty, you know in terms of what do they call it our philosophy expression in my head. | | |
|  |  |
|  |  | P21 |  | Yeah, I'm. I'm happy to send you our paper because for ransom, or at least we've come up with a whole taxonomy and we've sort of described first order harm. That's your organisation and the staff 2nd order. That's your patient in the hospital. Your student in the OR someone in your supply chain has a ransomware attack. And then third order. That's for us on a national level. That could be a societal national security economic.  So those are sort of the big order and it's really hard. It's really hard because the farther you move away from the immediate impact.  The harder it is to attribute it to a certain incident, whatever you see and the hard it is to keep a keep it, keep track of what's what impacts you're talking about in the 1st place. And often organisations have very, very little even for ransomware. Organisations have very little understanding of the harm that they're actually experiencing.  Yeah, yeah. | | |
|  |  |
|  |  |
|  |  | P21 |  | Yeah. And we've seen it in some of the schools where then you have teachers who said, OK, that's the final straw. I'm quitting because.  For whether that's not justified or not, but they had all of the teaching materials of the past 20 years saved somewhere that got lost in the incident. And yes, OK, in theory, that's the material of the school and anyone else and so on. But they said that's it. The university. The school didn't protect me. All of my teaching materials gone. I'm already overworked. I'm already annoyed because of COVID. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 313 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | This. That's the final bit. I'm. I'm done so and how partially people feel that.  And I they feel like personal injustice in that that moment.  But yeah, might might leave them to quit their job. | | |
|  |  | P21 |  | Right. So it has a particular.  So in terms of the impact, so it's this is this is.  Instead of, yes, I I've been thinking of the impact as being distributed geographically typically. But if you're thinking in terms of society.  There's there are laws of society who will be able to respond.  Easily or deal with it or whatever, and it's actually the the most vulnerable of society that are going to be most affected by.  These certainly certain sort these sorts of attacks because they don't know what to do about it, yes. | | |
|  |  |
|  |  | P21 |  | Yeah. Or or think of someone who, for example, might have. I mean, this is not CNN necessarily, but think of someone who.  A rape victim, for example, with that data in those in sort of legal files and so on. And then the law firm is is.  Is targeted by ransomware attack and that data actually that is quite different data being leaked from my pension statements or or something else. So I think there's and I mean it's also vastly depends on your on the broader political spectrum you can certainly quite easily imagine scenarios in the US where that kind of data health can so on.  Is being leaked in a state where there's recently been a very strict abortion rules that have been implemented. Some of that, so that sort of all plays plays into that. But I think certainly a disproportionate impact on those already vulnerable, that was the result from our research. | | |
|  |  |
|  |  | P21 |  | Places like the British Library facing that ransomware attack and they're taking months and months to recover.  Yeah, even something like that to this. And on one hand, just the library has such.  Extreme implications farther down the line for researchers, and so on and so forth. So we've seen that with some ransomware attack against universities. And then we're like, unable to conclude their research. And as a result, unable to receive further funding or something. So these sort of triple down effects I think can have quite long term implications for our society and its prosperity and well-being.  About the fact that you can't always immediately allocate it. | | |
|  |  |
|  |  | P21 |  | Yeah, I think that's certainly a risk to underestimate.  Some of those consequences. | | |
|  | |  |  |  | | |
|  | | | | | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 314 of 316 |  |
|  | | | | | | |
|  |  | P21 |  | But it can be an existential threat, that sort of business interruption. You can't manufacture, you can't produce, and so on. And as a result, you might have additional cost, loss of income, reputational harm and so on. But I think ransomware causes so many other kinds of harm that are sort of overlooked in that context. And that includes if there's ransomware attacks against critical national infrastructure, for example, the psychological harm that people face as a result of ransomware attacks. If your staff member working on this, it's particularly grave for it teams because they often feel personally responsible.  Work themselves into a burnout and then if you have an IT team that's on burnout, you know that they make worse decisions for your cybersecurity as a result as well.  At the same time, when critical national infrastructure is.  Implicated and we talk about it a little bit. Education doesn't fall into this, but let's assume a hospital or perhaps government structures that pay our benefits.  There you see a particularly harsh impact on those that are already vulnerable, which I think has societal implications as well. So you might think about the patient waiting for surgery. You might think about the benefit recipient of a local council.  You might think of those who are dependent on council housing or something like that.  And they fear particular consequences as a result of ransomware attack. If you're a multinational corporation, you have the the skills and the capability and the experience dealing with a crisis. If you're a local school, you don't. If you you don't, you just don't know what to do and you're kind of crisis is a different crisis that you're used to. You're used to being someone getting lost on a class trip or something like that, but you're not used to handling the cybersecurity incident and.  We found in our research that that kind of attack in terms of societal implications means that those that are already vulnerable feel more of their harm or are affected disproportionately. | | |
|  |  |
|  |  |
|  |  |
|  |  | P22 |  | Social care, increasingly, our assistance use remote monitoring to monitor the health of patients.  It's just endless, you know.  You know if if it goes down, you know.  They are sort of disaster of patients dying in care homes in COVID will actually be dwarf by the care patients in care homes dying because they're not being monitored. | | |
|  |  | P22 |  | You | | |
|  |  | P22 |  | And electricity is the new oil. If the price of electricity, you know it used to be that people talked about the price of barrel of oil. They not now talk about the price of a kilowatt of electricity. And that's the sort of indicator of economic help.  And you know.  Were we worried when there was a shortage of oil? Yes, of course. There was the world crisis. You're like in the 1970s and you know, everybody in the stage trying to dump all their big cars and buy volkswag. | | |
|  |  |
|  |  | P22 |  | Yeah. So we are so dependent on electricity.  And telecoms is dependent on electricity. | | |
|  |  | P22 |  | Well, you know, try to yes you know because you know if if the electric well we are actually in an area where the electricity goes off maybe once a month for half an hour and you just have to reset the clocks you just have.  But sure, if so, we did a lot of work with the xxx, who's to share that.  As as his nightmare that if electricity, electricity in some areas of the UK went out for three days.  The food stocks of the UK would be shot because of lack of refrigeration.  And you see there would be food riot.  That that is his background worry. | | |
|  |  |
|  | |  |  |  | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 315 of 316 |  |
|  | | | | | | |
|  |  | P22 |  | And that's one weakness, of course, of the.  Of the move to full fibre.  Whereas the old landline, once it's on the main's electricity, they have their own supply.  So we've become more dependent on electricity yet again by going to, you know, BT wouldn't let me have my old phone. I have to have a new crummy little phone. Yeah, because I've gone to full fibre. | | |
|  |  |
|  |  | P22 |  | So you know, there is really.  Not a workshop for a couple of months. London Borough Council's last week, and we were thinking about, you know, whether any of them have services that weren't dependent on electricity and, you know, so Richard Waste Management said, well, you know, my my trucks are electric. | | |
|  |  | P22 |  | And yeah, the compactors are, but most importantly the scheduling stuff and paying my staff.  Yeah. And you know, if they don't get paid, they changed. Get a bit crossed. | | |
|  |  | P22 |  | And so talking to the chief architect, I think is called at British Airways.  One of the big problems was finding a backup cloud for some of the places where he had to have data centres because obviously it's a wide worldwide network and it goes to some, you know, goes across the Middle East and so on and.  But they had built into all their thinking that would be a resilient cloud, so the applications assumed everything was going to keep working, so he couldn't. He wasn't, didn't have the budget to build into his applications, ways of checking if things were failing because the assumption was the cloud would keep working. | | |
|  |  |
|  |  | P22 |  | Well, it's it's connectivity.  But the the.  No, I can't use the phrase in the wood part, but the the lurking danger that xxx always brings out is that so much critical national infrastructure is built has legacy systems in and they were built to certain standards in terms of, you know, data checking at the front end. And you know now they're being bolted on with lots of add-ons that are brought in from all over the place.  A lot of those systems do not have the same extent of verification of data quality at the front end, and that in fact is the source of a lot of cyber attacks that you know the data checking at the front end isn't happening. And you know there are components built into all sorts of devices that are used in critical national infrastructure that have known vulnerabilities that have been.  In the software.  Incorporates into 260 manufacturers, devices and are now 20 years old and are still there, so there are lots of devices with built in known vulnerabilities, but you know it's not a priority to sort of pull them out because they're working OK, hence the need for AI to record and analyse transient almost failures.  Because we know that there are these buggy devices, these vulnerable devices, these faulty devices in there operating, you know almost 100% but not quite.  And also subject to cyber attacks, because you know, if you've got good enough defences at the front end, the cyber, the, you know, malignant attacks. Sorry, I'm. | | |
|  |  |
|  |  |
|  |  |
|  |  | P22 |  | But it's the electricity's out. The telecoms is out, isn't it? | | |
|  | |  |  |  | | |
|  | | | | | | |
| Formatted Reports\\Report Extracting R1 Coding | | | | | Page 316 of 316 |  |