# CONTEXT

**Description:** General Comments about Context of CNI

<Files\\P11R2> - § 2 references coded [3.05% Coverage]

So the kinds of CNI context and sorry, I haven't really thought about this, this is going to be off the top of my head. What did I expect to see in CNI context.

The impact of climate change is changing the nature of our critical infrastructure. Our electricity systems in particular, are becoming.

Decentralised, or rather, they're no longer.

Central generators with largely passive.

Users of energy there's there's a lot more local micro generation going on, which means actually the grid is is no longer a series of.

Arrows pointing in One Direction. I suppose that's one thing I think another thing is.

I'm just going to call it the general automation of of the C and I and the C and I is becoming and and it's only slowly becoming because everything has an asset lifetime measured in decades, so it takes ages for this stuff to happen.

And when I read this, I thought commercial drivers well1.

**Annotations**

1 commercial drivers well, yeah they are operated by private organisations, so that was my reaction.

## Question: Commercial drivers

**Description**: CNI are operated by public and private sector organizations; industry’s commercial, innovative visions will influence CNI technology strategies and their implementation.

Totals

No Opinion: 2

Strongly disagree: 0

Somewhat disagree: 4

Somewhat agree: 8

Strongly agree: 8

### P3: Strongly agree

### P4: Somewhat agree

So commercial commercial Dr is C and I are operated by public and private sectors and if it's influencing, I've said somewhat agree.

Well, yeah. But I mean, it's always been like this really. I mean you've you've you've always had the companies and you've had the supply chain, the supports it, so.

Yeah, I I I did. I did say somewhat agree rather than strongly agree because on one hand it is hard to share tacit knowledge about how stuff is done. But in but a lot of development knowledge you know how to programme in Java or programming, whatever the, unless it's a really esoteric language, you know, generally exists. I can't learn in O'Reilly and get a book or do the stuff.

### P5: Strongly agree

Absolutely. I think in the in the US, we are much more.

Industry driven than we are government driven for a lot of our critical infrastructure. And so that from my perspective, yeah, I think there's a lot of influence from the private side into the public side.

So I would strongly agree with that one.

It how and I and I would say that some a lot of the innovative visions and influence does come from our industry folks.

It really doesn't come from government, typically.

I mean, if I look back at history, I can count on one hand how many times the government has notified somebody in the country and this is from hearing from them, the utility folks and people who run these things.

That they were given some information saying, hey, you might want to consider XYZ.

And sometimes they do, sometimes they don't. But I think for the most part, it's driven by.

The industry private sector.

Interesting. And does that result in?

I'm wondering if the regulation is really the building of consensus.

Or whether actually you industry's mostly doing it and then the regulation comes later, if it comes at all.

### P6: Strongly agree

### P7: Somewhat disagree

It's an interesting one day the the first one.

Umm.

I mean, I wouldn't say I, I I disagreed to the first one, but to what extent?

Industry, like vendors, can can influence more than the sort of context of of CNI, which kind of push pulls back. If you like. I don't, I don't know. So that's definitely the sector. So I'm looking at there is less, less innovation, less accelerated innovation if you like and more sort of.

Legacy.

So I think I think I'll put some somewhat disagree.

### P8: Somewhat agree

### P9: Somewhat agree

Yeah. OK. So yeah, I think I think industry, I think industry is pursuing ways to do it differently.

And I think, you know, maybe not at the sort of necessary the financialization thing is a major distraction. But when we talk to strategic leaders and we talk to innovators, they are really actually quite interested in the changes they have to make to meet the energy transition. So they are trying to innovate. Yes, I mean, good engineers don't turn up to work to get paid. They turn up to do good engineering.

And I think I think they're trying to do that in the face of everything else that's going on. So there is genuine innovation in, in the industry, in the industrial sector allowing that innovation to be rehearsed, allowing it to have a have a go is kind of hard. The the risk profile isn't perhaps what we might hope it would be. So finding a way of creating regulatory or geographic or financial sand pits to enable these engineers.

To try things differently.

So there's things like that I think do matter and I think they they do. And the CREDO project in digital twins that was done down in East Anglia, again we're going to try something a bit different. Oh, turns out the reasons it's difficult aren't the reasons we thought it's other reasons.

### P10: Somewhat agree

I'm just not sure of the the commercial drivers in in you know CN is not my not my thing but the commercial drivers.

I think they they they seem to get.

And let me try and find a coherent way of putting this. My sense is that commercial drivers are sort of part of a bigger discourse, which is often driven by government. For example, the the, you know, the AI for innovation, kind of White paper. So I it's almost like the the discourse and the narratives around around commercial. And I've been slightly poisoned is too strong. But they have been polluted.

By that, you know, pro in a pro innovation pro.

Commercial, you know.

It's, yeah. Sort of. Arms race around various kind of technological invasions. So that's my my sort of equivocation around commercial drivers.

The kind of politically most you know, it's a sort of political hesitancy, I think.

Yes, I think I understand. So you're so you're concerned that they're not?

So it's not industries, visions, these visions are actually coming from government really this this kind of commercial innovation sort of thing is it is, yes, yes.

Yeah, I think so. I mean, yeah, exactly. I mean, I think I don't know. Yes, I think I think it's, I mean and it is this, you know it is this, this kind of government's, it's rhetorical and discursive. I'm not sure of the of of the of the strength of that, that sort of proposition otherwise.

### P11: No opinion

And when I read this, I thought commercial drivers well.

### P12: Strongly agree

### P13: Somewhat disagree

Yeah, I I I I'm somewhat disagreeing with the fact that commercial organisations will drive this forwards basically.

I think I think I think probably these challenges are so large that actually.

It's going to have to be state driven solutions.

And that that doesn't mean ultimately it will create commercial entities, but it's actually the innovation. Well, I don't think be driven by the commercial sector, that's not how to withdraw the parallel when it's thinking with the creation of the Internet.

And 60s and 70s.

As a resilient system to basically enable communications to continue in the events of nuclear attack, that's a classic example of this kind of resilience, isn't it?

That that was government funded so.

Yeah, yeah.

Probably I think there's a commercial opportunity there, yeah.

Yeah, and only the government could probably have done it. Or American Government could probably have done it. Yeah, that's that's an interesting one. So. So even if it is done by organisations and I'm sure the Internet was, it'll be done by organisations in response to government prompting rather than. Yeah, yeah. Rather than because they think it's a nice idea. Yes. Yeah, yeah, yeah. Interesting.

### P14: Somewhat disagree

Commercial drivers C and I are operated by public and private sector organisations.

I was thinking here.

First and foremost, and this is from experience.

The sorts of major.

Industries, the primes who operate the CNI are remarkably.

Uninvative.

That I know for sure.

They are not innovators.

Is something that's developed since we last spoke. I've I've run a really interesting.

Project, which, unlike the thing I sent to an electromagnetic environment.

I don't because it's been done for government and nothing's been published to my knowledge. I don't think I could sort of share you any documentation, but we've been just exploring the whole issue around how can we improve cybersecurity. We had that discussion about improving cybersecurity behaviours in the critical national infrastructure.

And one of the really.

He, he, he.

Insights that emerged as talking to a range of.

Non government experts. Is this a sort of tragedy of the Commons that's going on?

Those people who suffer from cyber security failings.

Don't aren't necessarily those who are accountable for those failings.

And therefore there is this mismatch between if there would, which is why you look further down the road somewhere in your list. I say 100% agree strongly agree we need regulation.

I suppose it's true that industry's commercial drivers will inform how it behaves when it comes to critical national infrastructure and cybersecurity, but it will be in unhelpful.

Ways, because there are often not the commercial drivers for them to actually make a difference that we feel there should be.

Well, that's. I'm always tempted to say that there are there are large numbers of examples.

Where over and I'd have to go away and reflect because some of those examples might have come to me through sort of.

Sensitive, sensitive conversations.

Off the top of my head, no. But if I come across something, I'll let you know.

### P15: No opinion

### P16: Strongly agree

### P17: Somewhat disagree

you don't agree about the commercial drivers

I don't think commercial influence the the the CNI technology kind of strategies because I don't think.

People understand CNR that well in terms of a security point of view, so let alone the commercial aspects of it. I think it's more led by spin outs from people who've worked in C and I. So I'm an example of that or.

Where existing companies or service providers are looking to.

Kind of gain a foothold into the market, so they will develop innovation in that sense. But I think it tends to be innovations driven by those who understand the problem, not necessarily. There's a collective thing going here in the industry, you know, shall we sort of open it up a bit? It is getting a bit like that, but I think it's more focused in, in, on a in that perspective, if that makes sense.

### P18: Strongly agree

### P19: Somewhat agree

I think people would like is investing in it.

You know, I I phone right right from the start and I writing about speaking about

The companies working

Money management

Too much and when

Leading a directive to profits with companies in design

profit is something I I can understand why they want to

Make enough profit to to keep going.

Somewhere

Yeah, anyway, but it does it does impact some of the

Some of the attitudes I think.

Particularly when particularly when we're talking about National infrastructure.

We're talking about. Things that are essential so maybe there are things that are they're

slightly more important than whether the company has to get

Critical in Crystal National infrastructure, because some of it at least some of it is is

controlled by private companies.

So I think again relating that to some

Questions that I think is a is a

A difficult issue to solve.

### P20: Somewhat agree

Yeah, I do. Yeah, I do think private private sectors commercial in, in innovation revisions do influence somewhat implementation.

Longevity of software it's as I, as I said to you, it's it's, you know, software is a thing that doesn't stay static, it gets updated a lot.

And I think probably the preserving developer knowledge over those time frames.

Yeah, I mean I I think that if you're if.

### P21: Strongly agree

### P22: Somewhat agree

### P23: Somewhat agree

### P24: Strongly agree

## Question: Longevity of software

**Description**: As infrastructure, much of the software is long lived: up to many decades. It is hard to preserve developer knowledge over those timeframes.

Totals

No Opinion: 1

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 10

Strongly agree: 9

### P3: Strongly agree

### P4: Somewhat agree

### P5: Strongly agree

### P6: Strongly agree

### P7: Strongly agree

Yeah, that's definitely the longevity of Software's definitely I.

Well, a hinderance in modernization if if that's what we want to do.

### P8: Somewhat agree

### P9: Somewhat agree

So I was sort of caught on this one because.

As infrastructure, much of the software has long lived, but it doesn't have to be. That's a choice that we're making.

We, we you could, unlike infrastructure, you've actually poured concrete and you've put your pipe in. I had a fascinating conversation with some colleagues in another engineering company who are raising the question around government integration over this. If you're digging a giant trench, say, just say between London and, I don't know, Birmingham, maybe even Manchester.

And and you knew that you knew you had a water problem in London while you were digging that trench, wouldn't you think? Why don't I stick a major water main down it so I can bring water down from the Manchester Ship Canal rather than having to dig a new reservoir in Buckinghamshire?

Or I could stick a major power interconnect underneath that rather than run cables all the way across East Anglia.

But I've got three different departments there planning three different solutions to three different problems. When there's one major national infrastructure project where they should have been put together.

Once you build these things, they are really, really hard to change software, isn't it? Shouldn't be hard to change.

But we tend to leave it either for safety reasons or for development reasons, and what we ought to be doing is going in and going, yeah, we can refresh the software. I mean, I have to update the software on my kit every every Tuesday, right?

How often do you want me to do this? Every Tuesday. Well, it takes six months to recertify. How do I square that circle? There are. There are real challenges there, but software shouldn't have to go through that longevity problem. That's a choice we've made.

### P10: Strongly agree

### P11: Strongly agree

That longevity of software, yes, I completely agree, and in fact I was at a plant where, as I recall, a good software background. So I was a VAX VMS 750 systems manager sometime many decades ago, and I came across a lot that is still using one for a critical function.

Yes, yes, and VAX VM. Well, it wasn't the 7:50, but it was a VAX and it was running VMS.

And there were on the same plant. There's also an NT4 box that's to some extent doesn't surprise me as much and it's nothing like his old. So anyway, yes.

### P12: Somewhat agree

### P13: Strongly agree

### P14: Somewhat agree

### P15: Strongly agree

I would consider placing this defintion para first in the list, as it is the main starter position - what IS CNI? And why does that matter if it influenced by changes and uses of software?

### P16: Strongly agree

### P17: Somewhat agree

Longevity somewhat agree.

Absolutely. Yeah. Yeah. I still see software that's written in the 60s still operating. So there you go.

And I think even in today's world, you know, even software that's developed today that's deployed, you know, I work on like we do a lot of work in rail and obviously nuclear has a similar thing the the asset lifespan of them tends to be like 4050 years. So I won't be surprised even if in today's world we've got more, we've got more language than we had 50 years ago. But I ~~would~~ won’t be surprised if we still see those some of those languages. Go about

About any sort with ~~cobalt~~ cobol in America recently with a lot of the finances a couple of years ago, the need for it. So yeah, this is a given really that one to be fair.

### P18: Somewhat agree

Yeah. So I, yeah, if it a lot of these are predicated by if it's done properly, yeah. So if you, if you do software software properly, then you should, you should be able to, you know maintain it over a long period of time. And we've got examples of that. So but you need to do it properly. So reengineering it is very difficult. But if you but yeah, if you do engineer it properly then you're more likely to succeed on that.

### P19: Somewhat agree

### P20: Somewhat disagree

OK, yeah, no problem. I think for sure is long lived.

A lot of annoyance.

Is much of the software long lived? I thought I would suggest that it's updated and modified fairly regularly. It depends how you're defining long lived, so I think I might somewhat disagree with that statement.

But is it? Is it the first bit or the second bit you want me to agree or disagree with?

Development knowledge over those torn primes.

Yeah, I do. Yeah, I do think private private sectors commercial in, in innovation revisions do influence somewhat implementation.

Longevity of software it's as I, as I said to you, it's it's, you know, software is a thing that doesn't stay static, it gets updated a lot.

And I think probably the preserving developer knowledge over those time frames.

Yeah, I mean I I think that if you're if.

Yeah, yeah, I'd yeah, I just, I don't know. Again, I it depends what software you're talking about, what functionality is. But but the you know the very premise of software is it's easily update or should be easily updated and modified. And people are aware of how that's done and they're aware of the vulnerabilities in previous iterations of the software and and what have you.

You know, maybe that there's a lot of kind of legacy software being operated in these sectors still, but you know.

And that obviously has been a problem.

But yeah, yeah, I guess I somewhat disagree with the premise of the questions.

### P21: No opinion

### P22: Somewhat agree

### P23: Somewhat agree

### P24: Somewhat disagree

OK. That, that, that could happen with every.

Type of knowledge, isn't it? Like if there's not a proper?

Change, change management, change, change control. I think it's the name then, OK.

So it is hard to present. Well. Somewhat disagree. I think it depends on how.

## Question: Definition of CNI

**Description**: Definitions of CNI vary considerably, from ‘sufficient to recover from nuclear attack’ (UK 1950s), to ‘anything politically sensitive’ (USA currently). The current UK definition is, roughly, services in 13 sectors where threats include major loss of life, casualties, economic or social impacts; or impact on national security or state functioning.

Totals

No Opinion: 1

Strongly disagree: 0

Somewhat disagree: 1

Somewhat agree: 10

Strongly agree: 10

### P3: No opinion

### P4: Somewhat agree

It's interesting, I I can't say I'm that surprised about what came up.

But then again, I don't know what NCSC are looking for. There's a lot of talk about C and I and resilience.

Then and some of the hardware NCSC wanna sort of put on on CNI and I think that's that's what's found its way in into our particular sector. People have thought, you know, people have thought, wouldn't cherry be good for that sort of that sort?

I'm come across cherry.

Oh, wow. You're gonna you're gonna. You're gonna need to keep up with what's happening. So cherry dspd dot text. So go to Dspd dot tech and you'll you'll find out. So this is the digital security by design programme, and I'm sure you've you've heard about digital security by the time.

It is, yeah, it is well.

Definitions of C and I vary variably. Consider. Yeah, I I I think they do vary. It's the I don't know what the flavour du du du jour is these days. For what it is and everything seems things seems to be getting added to it rather than away from it. So it's plausible that the number, the number of things acted C and I will go up rather than down so.

### P5: Strongly agree

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

I do agree with that. I'm just I may agree with the UK definition. I'm not the USA definition. It's definitely not. I think UK is the best definition to be honest, because I know how Germany is defining it and so we need UK really nailed it in terms of their like understanding

### P9: Somewhat agree

Yeah, yeah. I I I think it that it's it's good that we made that. The reason I somewhat agree is I think the actual practical definition in the UK is anything that puts a junior minister on the front page of the Daily Mail.

Because that's what's actually driving the decision making in the engines it we would like it to be. But the truth of the matter is, it's critical if you think a minister is going to ship bricks over.

### P10: Strongly agree

### P11: Somewhat agree

Oh yeah, sorry about Mt 3.5194. Right? OK. Definition of cni.

I think the interesting point.

In the CNI definition is that.

The CNI, if we go back to early Victorian times, didn't even include running water and it certainly didn't include electricity. And so over the if we're looking at a sort of if we look in 50 decade slices.

What we expect and rely upon on the day-to-day basis changes and at the moment what's changing is our reliance on network technology or you know the Internet.

It'd be interesting to think where's this going, because if I look at it in those terms, the only big change I can think of is is networks information systems.

### P12: Strongly agree

### P13: Strongly agree

### P14: Somewhat agree

### P15: Somewhat agree

official UK Definition is from here: 'Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a) Major detrimental impact on the availability, integrity or delivery of essential services - including those services whose integrity, if compromised, could result in significant loss of life or casualties - taking into account significant economic or social impacts; and/or

b) Significant impact on national security, national defence, or the functioning of the state.'

‘services in 13 sectors’ is insufficient a description of a critical national infrastructure. It is also about the impact that the loss of those assets would have on the functioning of UK society if they were disrupted.

Yes. So broadly, I think you're you should have said the UK CNI definitions vary and in the UK it's this, but actually that I think that sentence doesn't really do it very much justice it. All it says is CNI are 13 sectors.

And the threats to them include lots of life, but that doesn't describe what acni is like. At no point have you described what Acni is in in there, and I think it's quite important to your whole project is about CNI to be clear about what it is that you're looking at 1st and I think also because of the context, if you're trying to look at what the.

The the impact is about the loss of those and therefore.

That that's why they're interesting. They're only critical because if we lost them, they would cause such a big impact.

And so I think that is important and I would almost put that at the top before you're even starting to say about how they commercially work or how software integrates into those systems. It will be more useful perhaps to think about CNI first, what it is first and why it's important in the context of this.

No 'cause, it doesn't actually say if it doesn't really say what they are there and and therefore that's also the interesting thing is if you look at different organ at different countries, definitions of C and I, they they different sectors are are accounted for or not accounted for.

And sometimes that is because those sectors are manifestly important for their like their economy and aren't for other industry, for other countries. And so it is important to take that into account.

And also like in the UK, it covers local government and emergency services.

Which which there might be sort of different definitions. And then if you start to think about AI in the context of those things rather than as as I kind of get the impression, most of what you've been talking about is people in the nuclear industry or in sort of high risk industries. But actually the provision of law and order and and public services is also very critical. Like everybody gets very irritated. There's no if the bins aren't, bins aren't collected within three weeks. And actually like, if you look at other countries where.

They have had major loss like relatively sort of.

How to say like I, I I Greece in Athens when all the bin bin operatives went on strike for four months and they just had rotting garbage in the like piles of rubbish and stuff in the city, like those things that also disrupt?

Yeah, like all of these things have got different things of of scale and duration and things like that. So I think it's important to note that it isn't just these kind of like obvious socio technical systems that you're talking about.

### P16: Somewhat agree

Yeah. Well, I was just gonna say that the reason for the somewhat is that.

We still tend to present CNI as as a as a list of different sectors, and I think what the pandemic showed us is maybe it would be useful to also think of it in terms of functions. So you might have, you might end up with having.

Companies or systems that are not integrated technically in the C and I.

List of entities. But because they are serving cnis and I'm thinking for example of cloud providers, although they are technically under telcos but they are not telcos.

But they're serving now the financial sector. So even if the financial sector is defined as financial institutions, if they're cloud provider.

Collapse and they collapse as well.

But cloud providers are not yet.

Formally recognised as CNI. So that's why I was some somewhat yes, the definition is about sectors, but I think the the, the Americans have started to list functions that are serving C and I and they would like to see a, a shift towards thinking of C and is as interlinked functions and more than static sectors. So that's why.

### P17: Somewhat disagree

definition. You didn't agree that didn't agree

So I think.

My understanding is the way it's classified. I sort of disagree with with the potential of what's the classification or definition for for CNI because.

I think the issue at the moment if you look at nisd and you say right, NIST, it sets out a criteria for what is deemed C and I critical national infrastructure and therefore needs to comply with NSD. If I was to spin it on its head a bit and so actually if I've got again, I'll take it from experience as I'm talking about the rail sector here. So if I've got some rolling stock, which is basically another word for trains.

The OEM, the, the.

The system, it's great, or the manufacturer of that train is potentially got to do something about it, but at the point of time when they build the train, it's an I asset. It's only when it's going into service it becomes acni asset, but obviously those buying the asset are aware of this. So they will put requirements in the contract now that kind of forces this chicken and egg thing because the Oem's not obliged to unless it's contractually told to and they won't go above their way to say.

We'll just put this in because we feel like it's the right thing to do. So that's the issue. And then I think the bit, I see it more is on the supply chain. So in theory, it's like I know you could argue how fast the supply chain. So from a customer which could be a public sector organisation to do OEM, there's a direct relationship there and that's quite easy to map. But there may be several supply chains down the chain of of ribbon and quite a lot of that even though they do get pushed to do security.

They're not required to.

Be classified as a CNO, but The thing is, is we've seen it supply chain. We've seen it just be recently with the NHS. You know, there was a company there that was responsible for the the IT systems that looked after the blood bank, right?

It obviously wasn't classified as CNI because if it had been, I would imagine there would have been a lot stranger.

Procurement issues around it and assessments done beforehand before that company, clearly it's not today. Therefore, that's the definition of that's what's not been defined. I don't think by C and I.

### P18: Somewhat agree

Well, we work. Yeah, I wouldn't. I wouldn't have a problem with that. I mean it, it ends up, you know, the approach to risk I always think should be dynamic, not static. So, you know, over time it will, it will shift, aren't it? So you know somewhat, but as of as a starting point, you know, it's fine. Yeah.

### P19: Somewhat agree

### P20: Somewhat agree

I believe that should read 1960 is not 50s.

So you wanting me to say, do I agree that the UK definition is services in 13 sectors?

Somewhat agree. I guess I knew it was 128 something. I'll need a minute. I accept this.

Definitions. Yeah. If it's about, you know what we should be covering, I think probably the UK has it about right. As we've discussed before, there's this debate about how wides do you include critical infrastructure to be and you know, talking about.

Democratic systems and processes, for example.

You know, it's the debate about if you broaden it then does it become impractical to actually do something about, conceptually, definitionally and in terms of regulation?

And organisations, yeah, I think it's differentiated across those sectors as I've described. So yeah, I think that that's what my my comments would be on that. I hope that's helpful.

### P21: Strongly agree

### P22: Somewhat agree

### P23: Strongly agree

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.

Well, that's inch. That's quite a distinction, isn't it? The sort of the so, so the 20%, that's most important is actually in the eight that they, yeah, is actually in the public sector for example, what are they thinking of that?

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.

### P24: Strongly agree

## Question: Only respond to regulation

**Description**: Organisations in highly regulated sectors, such as nuclear, energy and health, tend not to be proactive, but wait for regulation to define their response to risk.

Totals

No Opinion: 2

Strongly disagree: 0

Somewhat disagree: 6

Somewhat agree: 11

Strongly agree: 3

### P3: Somewhat agree

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.

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.

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.

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.

### P4: Somewhat agree

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.

And and and I think is expected, people would if things go wrong, people would want to hope that there is a regulator there.

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.

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.

Because you can't trust industry on their own to to do stuff. Secondly, is people might try and game.

Things I mean and the Boeing 737 Max thing is an example of of of of where that might happen, yeah.

### P5: Somewhat agree

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.

### P6: Strongly agree

### P7: Somewhat disagree

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.

And and that it it needs to come from them. And I think I think operators understand this.

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.

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.

One way power you know? Yeah, yeah, yeah, yeah.

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.

Whatever. Whatever the frame. I mean, I'm. I'm speaking in general, so.

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.

### P8: Somewhat agree

### P9: Somewhat disagree

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.

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?

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.

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.

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.

### P10: Somewhat disagree

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.

### P11: Strongly agree

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.

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.

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.

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.

That being, no other issues, yes.

There have been nothing else. There is nothing else. There is no other starting point for the process of design.

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.

### P12: No opinion

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.

### P13: Somewhat agree

### P14: Somewhat agree

### P15: No opinion

### P16: Somewhat agree

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.

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.

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.

### P17: Somewhat agree

And you somewhat agree that they only respond to regulation.

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.

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.

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.

### P18: Somewhat disagree

Organisations are re regulated, such as nuclear, yes.

Look at what? Yeah. So in ONR I was head of innovation.

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.

OK, I see. But it's good to put some things that are provocative in. Yeah. So that's that's that's good.

### P19: Somewhat agree

### P20: Somewhat disagree

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.

### P21: Strongly agree

### P22: Somewhat agree

Exactly

Absolutely yes. But again, I mean, you know my scope is, is is CNI and is these these fairly regulated in things, yeah.

But telecoms isn't telecoms is not very regulated really in that way, so they might.

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.

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.

### P23: Somewhat disagree

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.

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.

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.

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.

### P24: Somewhat agree

# TRENDS

**Description:** General Comments Trends.

<Files\\P15R2> - § 2 references coded [0.93% Coverage]

Oh, also just in terms of if you're looking to group them, it seemed to be that 3/5 and six were all about people you'd like. People using the technology.

I increased digitisation in end users depend on it more to do things and system operators will be interacting with that in a different way. So I thought it might be more useful to put them together and also just change the order which would be 365. Ultimately I think yeah.

Yes. Otherwise it's just kind of like a OK, So what?

<Files\\P22R2> - § 4 references coded [3.96% Coverage]

Increasingly, the importance of this stuff to society is such that.

It it the real concern is the impact on users and the resilience of the overall thing.

That is the the overall packaging and a lot of.

And so asking what contributes most to keeping the puntus happy like they have their electricity is the important question for this stuff.

I mean, it helps. It's a little harder to define because a lot of the things that are not working around health are to do with, you know, administrative systems rather than basic underlying software. But there are also questions about, you know, I mean, I refuse to have my personal details on the NHS.

In information sharing things, so I don't think their security is good enough. I really believe it will be useful if everyone put their data on there, but I don't think their confidence to look after it. So there are questions there around. You know the data structures and so on. But that's I don't think data structures are the big issues in health.

I'm not sure whether it's, you know, lack of data sharing, but there are no comments about any of that that relate to health. Nobody seems to pick up the health sectors, but.

Yeah. I mean it's I, I would have thought if you made it related to the communications in energy sectors.

With a side comment that the nuclear sector is going to be changing in characteristics so much over the next 10 years.

That it needs to be nurtured as a sort of legacy industry. But yeah, it's a special case that might help you with some of focusing on some of your recommendations or some of your finding.

## Question: IoT and other next generation technologies

**Description:** By 2040 there will be extensive use of Internet of Things (IoT) technology such as smart sensors and edge sensors, as well as Digital Twin and Cloud based technologies.

Totals

No Opinion: 1

Strongly disagree: 0

Somewhat disagree: 0

Somewhat agree: 6

### Strongly agree: 15

### P3: Somewhat agree

I mean, you, you're you're, you know, you know, this sort of thing, Charles, I guess looking at futures and stuff. But you know, what are we gonna be talking about in 2040?

Is it? Are we still going to be talking about IoT and digital twins and cloud or is it going to be something else because that, you know, that's quite that's what, you know, 15 year time horizon.

Yeah, maybe, maybe, maybe just this sort of counter out my kind of.

Or sort of counter my my own argument there about.

About technology.

And and and sort of. OK, so a couple of weeks ago, I was involved in a training course.

For the UK, for the UK Nuclear civil nuclear sector.

And operating under Chatham House rules and stuff like this. So I guess we need to be a little bit careful but.

This is not particularly sensitive, so one of the instructors there was working at. What's supposed to be the most digitally advanced.

Nuclear facility, right. Well, yeah. This is a new build.

OK. And he asked this sort of, you know, pointed question, you know, what's the sort of vintage of the technology that exists in in this nuclear facility? And the Long story short is it was, you know, the stuff was sort of established and designed in the mid 90s.

You you could imagine that accelerating somewhat with some of these new builds and stuff, but still there's there's still gonna be a bit of a lag, right?

For various reasons, but yeah, so so, you know, maybe 24. Yeah, sure. Perhaps that's what we will be.

And but but the technology will have moved on again. You know what I mean? So in terms of the sector, you know, but but you know what's at the bleeding edge of of you know.

Sort of innovation in terms of technology might be further down the road, but you know perhaps we'll be kind of still dealing with digital twins and cloud technologies because of the kind of decisions we're making now about the way we design. And anyway, just a thought.

Yeah, exactly. Yeah, yeah.

### P4: Somewhat agree

### P5: Strongly agree

I absolutely believe there will be an extensive use of IoT.

That's like and for me, a no brainer. It's just keeps coming, coming, coming and we're gonna have to deal with it.

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

Are you telling me? Thank you by today's stand series off, which is not, yeah.

I definitely, especially in digital TV, we are using it a lot in our four stations and stuff. Even you know Fourier, I didn't know that. I didn't tell you. So for example for the maintenance activities and where things are. So in terms of improving the to the staff performance.

And to you and to sort of, for example, there's a lot of a lot of infrastructure are short of staff and you can't always give them the training like on the spot and digital TV can sort of help with that like in terms of general and how that you need to prepare the certain people and find a lot of data stuff I even provided.

I can't have this project, but one of the new projects which they are developing a new railway line in the UK. If you quit social my profile you will find out.

Was the lead person and I'll provide some data to the digital team and Gus about human factors. So things like for example, what are provided was requirements. So the requirements of what the staff would require, what the humans would require from a digital team. So it is definitely is there is being used right now. So by 20 to 40 definitely I mean to by 20 this project is up to 2035. I would say even even earlier than that I would say yes, so.

And it's my view just because I'm involved that it's a close based because they are, they are trying to understand the.

Requirements you see and like so this why they are coming to us because you know so they are done down that they are not going to get rid of him they just want to cope with the changes and you know the job changes and stuff and anyway yeah so this good question it should I've had I quite like this one build on it I would say it's good one the system complex the.

### P9: Strongly agree

### P10: Strongly agree

### P11: Strongly agree

### P12: Somewhat agree

General trend so IoT and other next Gen by 2040 there will be extensive use of IoT. Gosh, I am so conflicted about this because on one hand we already live in that world. On the other hand, it's like not that different from how it always has been. It's like kind of by a different name. I'm gonna say it's somewhat agreed.

### P13: Strongly agree

### P14: Strongly agree

### P15: No opinion

For what kinds of purposes - please can you give a couple of examples?

Because I think in particular, if you sometimes throughout this, you sort of seem to expect the reader to have a background information and things and you talk about things as if they're kind of like very well known. And I I think, yeah, again depending on the audience, you may need to be more specific or to sort of like give them an example to show them what that's like.

As I have no idea what digital twin means, I'm or at least I was sort of gathering it by the end of.

Yes, but in terms of not just an example of a digital twin, but like where will where will the use of IoT technology and digital twin and cloud based, like what kind of examples do you see them being used on in, in CNI?

### P16: Strongly agree

### P17: Strongly agree

### P18: Strongly agree

### P19: Somewhat agree

### P20: Strongly agree

### P21: Somewhat agree

Yeah, I think that it. For example the, the the use will increase. So that's why I generally agreed.

But then at the same time I sort of think by 2040 sometimes that seems closer than it actually is when it comes to changing a lot of technology.

Especially if you have sort of traditional infrastructure and so on. So that's why I thought, OK, yes, I agree to some some extent, but not I don't think everything will be completely different but 2014.

### P22: Somewhat agree

### P23: Strongly agree

### P24: Strongly agree

## Question: System complexity and interconnectivity

**Description**: By 2040, increased complexity and interconnectivity will make CNI systems more difficult to design, understand and manage.

Totals

No Opinion: 1

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 8

Strongly agree: 11

### P3: Somewhat agree

Yeah, I think that some of that as well is a little bit.

Related to OK, I think there are two things going on with with my somewhat agreeing with that.

Probably if you look.

Broadly across the sector, I would tend to agree, I would fully you know, so if you look at kind of energy systems that you know they're becoming, yeah, more interconnected, difficult to understand.

And all that kind of stuff. And I and I think you know.

Research is a sort of.

And you know, to maybe even AI, if I don't know, in the generalist sense I suppose, but you know we're we're coming up with tools and methods to understand that complexity or be able to manage that complexity. That's hopefully something that we're doing that's that's sort of kind of why I think it will be the case. However, I think for certain types of systems.

That will not be the case. I think. You know we there.

So in in in the kind of nuclear space they talk about quite a lot. They talk about this idea of a graded approach.

The security right.

Rated approach and basically I mean so this is a sort of general principle for nuclear security.

And and the idea. Well, yeah. So what it means is basically.

That you apply security measures commensurate to the risk to the.

Like reactor reactor protection, if that. If that function fails, it's, you know, the consequence is much more significant than and you design systems and apply security measures, security requirements commensurate to the risk.

But I think for the really safety critical systems that we're we're worried about.

I don't think we will have this, you know, complexity and interconnectivity that we're talking about, right, so I think.

So I think and and you kind of see that you see that in the kind of regulatory approach for example in the UK, right they you know, you have to kind of still.

For nuclear, at least, anyway, you still have to make a safety case a plausible safety case. Right? And and then, you know, you're not anyway. So that's why I somewhat agree. I generally agree that there is this sort of increasing complexity and sophistication in connectedness. But I think for certain things, probably not.

### P4: Somewhat disagree

Right, increased complexity will make CNI system more difficult design, understand and manage. Yeah. OK. So it's the reason that some somewhat disagrees. And if you said complexity and interconnected will make it difficult, I would say agree but it's the increased complexity because I don't think there's going to be that. I don't think the complexity is going to go up that much.

And I think that that was my and I think I've said this to and I think I made made the comment I've said this to a number of now it could be my interpretation of it. And if you tell me if you tell me what your interpretation of increased complexity is, I can take an opinion about whether that is really somewhat disagree or not.

What? But knowing people that work in this area, what gives me confidence is that if someone tries to pass off some technology to work in to get something test certified in that domain.

And regularly doesn't understand it, they they just won't pass it. They'll say it's not my job to understand your complexity, it it, it's your job. So.

So it so I I like it because you've got the regulator there. I think it's going to inhibit that increase that you mentioned. So that's why I said if it was this complexity will make it difficult. But I think the regulators is is is basically slowing things I think and in and for a good reason slowing things down now.

One of the things that's that we look at, I guess we in my current job is how we can make the certification process perhaps a bit more productive, a bit quicker. So it's not so slow. So if people do have ideas about how to use automation better.

Then we can make a decision about whether it's safe and secure or.

But no, there it's not a web app, it's not. This is not a business for us, for, for, for for startups, not to say start-ups aren't welcome, but.

### P5: Strongly agree

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

There we we can add to this. Obviously you know we make more vulnerable as well to you know both to the we talked about it in terms of the human error and also attacks. And so I would expend it like so I can write a whole paper about this particular sentence.

### P9: Somewhat agree

### P10: Strongly agree

### P11: Strongly agree

### P12: Strongly agree

OK, system complexity, increased complexity will make CNI systems more difficult to sign. You know I have no difficult to understand see design, understand and manage those are different things.

I think it could be radically easier to design and manage because we outsource it all to llms or whatever, but they might be for that reason much more difficult to understand. So I'm going to say strongly agree, no, I don't agree with 100%. I think the understand's important enough that.

### P13: Strongly agree

### P14: Strongly agree

### P15: No opinion

Even more? They are already complex and connected sociotechnical assemblages. Also using the word systems means we think of them as at some point closed and bounded when they are not

Oh, I think in #2 it was just around again. It's just sort of on the the wording, a lot of these seem to suggest that some of these things aren't going on now like by 2040 like this thing will have happened and we, but it's not like this now, but it's actually a lot of them. Those things are already happening and I suppose the the your point is probably that they will happen to a greater extent or the impact will be greater or it's more likely or any of those things. It doesn't sort of more.

Because all of CNI systems are inherently complicated, complex, sociotechnical things already, they they kind of were even 20-30 years ago. They're just becoming even more so.

And also just because I went to very interesting lecture on.

It was a guest lecture on systems and I thought it was going to be about system thinking and linking everything together and it was actually like, what are we doing when we use the word systems?

Which actually made me think lots about.

I'd refer to it later around actor network theory, and when you use the word system, you seem to suggest that it's like a thing that could ultimately be kind of pinned down on a 2D like nice mapping diagram. And then you put a nice boundary around it. And that's the thing that you're talking about. Whereas often these things are, they're not boundable, or if you have to bound them in order to look at them analytically, then you have to choose a scale that you're looking at.

Because all systems, when you look at them are made-up of smaller systems that work on in between them. So like if you're looking at even the energy network, you could look at different parts of that and then you could look at a nuclear installation, which would be one part of the system, which is also a system of systems. And then inside the reactors or systems of systems. And every time you look at it, it's slightly like a fractal. So it just gets smaller and smaller or it all becomes bigger and bigger. And part of that.

Yeah, and. And they're all interconnected and where you you have to in order to sort of be able to talk about things or or to analyse things you you kind of have to put artificial boundaries in and just to sort of delineate because you can't talk about Everything Everywhere all the time. So you have to put it, you have to put the boundary around it and talk about, I don't know the the communications system. And so does that or does that not include the Internet and only is it only telecommunications or whatever, which is something we come to later.

And so therefore, like in order to talk about these things, we have to put boundaries around them. But you have to and I think you have to acknowledge that you they are kind of artificial boundaries because the little tentacles of where systems go and they're not as neat as the word system kind of infers.

### P16: Strongly agree

### P17: Somewhat agree

you somewhat agree to complexity and interconnectivity, making it more difficult to design, understand and manage

Yeah, I I believe so. We we have an issue in that there's complexity now because a lot of people don't understand seeing our systems because it's an engineering LED industry and those that come into cyber tend to have come in from an IT perspective, the IT and engineering are very different. So that's complex in its own right today. But then if we're going to start to, I mean we're we're building IT systems to check into OT environment. So we're adding to that equation. So you know the landscape is going to get a lot more diverse and complex.

Interchanged in the future for sure. So yeah, it will be I think system complexity will increase with connectivity in, in the future that's that's sure.

### P18: Somewhat agree

Yeah, OK. System Complex 3 connectivity 3.1 increase complexity will make. Yeah, again this is these are all predicated on doing it properly. So if you did it properly then that might not be the case. So that's why it's not strongly agree or disagree. It's somewhat somewhat agree so. But you know there's no reason why you can't do it properly and you avoid.

These a lot of these risks.

### P19: Somewhat agree

Systems that were not core designed or designed together or designed to work together.

For a complex system to move people don't understand.

Feel that indeed is there have been periods of work on complex systems

and the last complex systems institutions.

They are relatively neglected.

It was a complex systems product that you feel that it didn't seem to deliver very much.

And again that probably made funders feel well.

### P20: Somewhat agree

Yeah, I mean I I think I'm broadly in in agreement that it will be more.

Difficult to manage CNI systems, but you know that.

I'm not too pessimistic that people can't do it in a way that they're explainable and and.

The the the design processes won't be can't be streamlined, and that the effective management processes can be put in place.

To manage that complexity. So yeah, I'm sort of.

Umm, I don't think automatically we should be thinking it's gonna be more difficult. I think that there's potential to manage that.

### P21: Somewhat agree

But then at the same time I sort of think by 2040 sometimes that seems closer than it actually is when it comes to changing a lot of technology.

Especially if you have sort of traditional infrastructure and so on. So that's why I thought, OK, yes, I agree to some some extent, but not I don't think everything will be completely different but 2014.

Yes, I see that makes very good sense and the same thing about interconnectivity, then yes. Yeah, a bit more difficult. But we're not talking about a huge difference.

OK. Yeah, system operators.

You've got a no opinion on system operators working through software rather than directly is that.

### P22: Somewhat agree

Then I think I achieve and it increase in digitisation and decentralisation. Yes, all sorts of clusters together, but the context is software is big, it's important, it dominates the reliability picture and complexity and interconnectivity drives the agenda.

### P23: Strongly agree

### P24: Somewhat disagree

## Question: Increase in digitisation

**Description**: Towards 2040, most systems will become software-controlled, to increase efficiencies, decrease costs, for data accessibility and to free up physical space.

Totals

No Opinion: 1

Strongly disagree: 0

Somewhat disagree: 0

Somewhat agree: 7

Strongly agree: 14

### P3: Strongly agree

### P4: Somewhat agree

### P5: Strongly agree

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

Well, again, not my full expertise. I think they will be something controlled, whether it's a software controlled or whether that you pretty much they can add this to class based technology part of software. Just what I'm I'm not sure nowadays what is the definition of software, it could be hardware this link to something else I'm not sure, but it will be definitely something software is related control to increase efficiency decrease call data accessibility and fill it up. Yeah definitely I would say yeah.

Yeah. And the other thing that which I'm not clear about here, so just to give you feedback, when you say systems in my mind systems are a little bit different than the than the infrastructure in terms of you know the system, the things that you can move around and lock infrastructure, other stuff you can't move around. So there is for example on the rail, you talk about the trucks, there might be software controlled as well, but they are not system, they are infrastructure in terms of definition. I somehow think this is.

### P9: Somewhat agree

No, I don't have major concerns. I think these are accurate descriptions of trends that we're likely to see. I think my my challenge again is.

There's, I mean, particularly when it comes to talking about the risks and when these trends evolve into risks. There's a point that Edward ~~Lukveck~~ Luttwak makes when he talks about strategy and strategy. Having layers when he talks about the technology level of strategies, people get really excited. Someone comes up with a new technology and says it's revolutionising everything. All bets are off.

These things are everything changes.

But when when they actually get deployed, it doesn't get deployed in isolation. It gets deployed and the the system changes around it. So we will see increased digitalisation of these systems. We will see increased complexity as they get woven together.

But that increased digitalization will come with increased deployment of physical systems and the increased complexity of connecting will cause there to be new mechanisms of simplification and management so.

Whether these things are good or bad depends on how we actually do them and how we react to them. So I think I think there's a, whenever I'm talking about risks and I get, I get really people get irritated by me doing it because I I I'd like to formalise a risk statement always as saying there is a chance that something happens with a particular consequence and if we haven't made the statement of the event and its consequence, we haven't fully expressed the risk talking about the probability of something happening is not talking about risk.

Talking about bad things happening is not talking about risk, it's the connection between the two.

And when we unpack that sort of probability and impact, we actually find, particularly in the conflict space, where we think there's an ad, there's a bad actor, we need to say, is there intent changing? Are the opportunities changing that changes the probability? Is there capability changing and is our system's resilience changing and that changes the impact some of those are in our gift, some of those are in their gift. So when we're saying these are trends, what they are is they're trends in opportunity that doesn't necessarily change the risk at all.

They're saying there's a bigger attack surface for complexity, but that's only an increased risk if the other things don't change at all, and they will change, they will change because because nothing ever goes into an isolation. So whether this actually makes the world better or worse is entirely dependent on the other things that happen at the same time, and hence hence it was more the more challenges like, yes, these are these are, I agree, I somewhat agree, because I think that's an accurate reflection of the increasing opportunity space. But I wouldn't express it that way because I don't think it's necessarily that conclusive.

### P10: Somewhat agree

### P11: Strongly agree

### P12: Strongly agree

### P13: Strongly agree

### P14: Somewhat agree

123 increase in digitalization towards 2040. Most systems become software controlled.

I just don't know enough about. I mean I could. I can clearly see there is merit in that.

But not enough of an expert in the systems to know.

If most of them will be.

Clearly it's a worthy objective on yeah. So I can understand that would be a strategic objective for the credit CNI to move towards. That's why I somewhat agree, but I can't strongly agree because I don't know enough about the subject.

### P15: No opinion

What kinds of physical spaces? As in to free up physical space on CNI sites which would otherwise be occupied by human operators?

You're gonna move like you seem to suggest that you're going to digitise as a mechanism to release space.

I mean it, it could also be a perfectly viable reason in in some limited circumstances. I think it was just the way it was phrased. It seems to suggest that it was relatively common. And I I suppose that makes sense for London transport or Transport for London because actually they are going to be pushed for space. But other other CNI sites and operators and infrastructure managers.

Won't necessarily have that kind of issue because they'll be in the middle of nowhere, where space is less of an issue.

### P16: Strongly agree

### P17: Strongly agree

### P18: Strongly agree

### P19: Somewhat agree

### P20: Strongly agree

### P21: Strongly agree

### P22: Somewhat agree

### P23: Strongly agree

### P24: Somewhat agree

## Question: Decentralisation of services

**Description**: Towards 2040, digitisation will enable decentralisation of the operation and delivery of CNI services. Remote communications, wireless and radio technologies will allow the dispersal of functions like electricity generation, including nuclear in the form of Small Nuclear Reactors.

Totals

No Opinion: 2

Strongly disagree: 1

Somewhat disagree: 4

Somewhat agree: 9

Strongly agree: 6

### P3: Strongly agree

### P4: Somewhat agree

### P5: Somewhat agree

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.

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.

### P6: Strongly agree

### P7: Strongly agree

Centralization of servicing.

Yeah.

I likely though the SNR or we we call them SMR small modular reactors, but yes, very good.

Charles: 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.

Well, Rolls Royce is pretty much into them.

### P8: Somewhat agree

. 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.

Yeah, the wording, the wording can be improved. Definitely, yes, yeah.

Yeah, especially railways here, the remote communication, wireless radio.

Small reactors because you mentioned this, I could say somewhat agree.

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.

### P9: Somewhat agree

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.

And that sort of undermines the clarity of the of the statement, but there will be dispersion of electricity generation definitely.

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.

Generally, if that makes sense, yeah.

### P10: Strongly disagree

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~~ dare I say safety critical in this space?

Yeah, I again, I think there's a political element to that decentralisation mode. Dare I mentioned railways.

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.

Charles: 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.

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.

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.

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.

### P11: Strongly agree

### P12: Somewhat disagree

Decentralisation will enable decentralisation, operation delivery. Gosh, I hope so. But I kind of doubt it. I'm going to say somewhat disagree, unfortunately.

### P13: Somewhat disagree

I I I'm not convinced that.

Remote Communications will enable.

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.

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.

### P14: Strongly agree

### P15: No opinion

This is important because there will be more sites contributing to CNI but each may be less individually critical.

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?

### P16: Somewhat disagree

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.

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.

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.

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.

Yes, yes.

Yeah. So services will remain very centralised in my opinion.

### P17: Somewhat disagree

you disagree about decentralisation?

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.

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.

Yeah, if we're worried about it, we centralise it kind of thing, yeah.

It's. Yeah, it's a go to kind of approach really it's.

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.

### P18: Strongly agree

### P19: Somewhat agree

### P20: Somewhat agree

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.

### P21: No opinion

### P22: Somewhat agree

### P23: Somewhat agree

### P24: Somewhat agree

## Question: Increased end-user dependency on technology

**Description**: 2040 will see increased reliance for consumers on software and machines to carry out and plan activities.

Totals

No Opinion: 3

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 5

Strongly agree: 12

### P3: Strongly agree

### P4: Somewhat disagree

So three increase in digit increase in digitization. Yeah, I mean I think it's about the same. I've only I've owned an iPhone now since.

2007 so where are we now? We're now 2024. I don't think how I've used it has substantially changed over that period.

So I think web services are generally more reliable. There are things I will do now on my phone.

That I used to do on on on, on, on, on, on, on on my laptop. But you know I I I wouldn't say technology is.

Fundamentally changed by my working life, even though I probably work from home. Well, actually, do I work from home more often than I used to? I mean, I I I moved job, but I think what's happened in the process of moving job is that academics are now more, more tied to to to the office. And I happen to be in, in, in, in a job where we actually can work a lot more from home. So yeah. So I think that's the reason why I've said somewhat disagree.

### P5: Strongly agree

### P6: Strongly agree

### P7: Somewhat agree

### P8: Strongly agree

Increase the reliance on software machines secure template and I think afterwards they will have to find a way to do this slightly different branch, you know all the data and everything. We go over the roof, but up to 40 I would say yes.

### P9: Strongly agree

### P10: Somewhat disagree

Not even with chatty BT? No. And again, this is this is what we've been doing and conversations. And I think again just that it's the reliance. I don't think that people are really keen on on there must be yeah there must be humans in the loop not we can't rely on it so that that that's my sense also a soft software is buggy most of the new stuff that's that's you know is coming out of is using libraries we still have you know real issues with unforgivable software errors you know.

It's it's I. So yeah, I don't see in this in, in this sector. Again the people are just too smart. It's it's it's it's kind of just just just to hand over stuff to something we all know is is is buggy and I don't see any grand visions like you know.

Digital security, by design, getting rid of that because we've seen that actually exacerbates the the software issues. So yeah, I I I don't.

Sorry, you, you, you said digital security by design, exacerbates the software issues.

I said actually it makes it worse. It so. So yeah, it makes it worse. So this is so whatever arm are, you know, are I forget that these these are being recorded. Charles I should I should be less libellous.

They will not be attributed, they will not be attributed to you and unless the work has been published, I will not. I will not pass it on to the person who is telling me that Morello solved all their problems in exactly the context you've just named. But if you have a reference, I would like to pass it on to that person.

Yeah, it's it's the the hype. The hybrid mode was, which is is. Yeah. And I've heard them be very confident. I've also seen.

Yeah, I will find out that he's presented. He's certainly presented at conferences, so there should be something in circulation. Yeah, I'm pretty sure I'll find out. Otherwise, you didn't hear it from me, right?

### P11: No opinion

I wasn't sure who this end user is. Are we talking about?

My wife, as the person who pays for our domestic electricity bill.

Yes, but is this a problem for? Is this a dominant problem and is it peculiar to the CNI? It just didn't? I didn't. It didn't resonate. I didn't know why it was.

I still don't. I still don't understand the point.

It's important in a wider context that I can't do anything about it without the Internet anymore.

If that's what it is saying, then.

I think I would have put it more to do with the fact that it's echoing the earlier point that society now considers the network the Internet.

To be an an essential service. So I worked in the Cabinet Office about, oh, I know, 1012 years ago, and one of the discussions going on then in terms of the government's position on cybersecurity generally was whether.

It was so some people were saying that access to the Internet was becoming a human right.

And and obviously you get. You'll get tangled up in the politics of it, people saying they haven't even got running water in some places. But but I use it as an indicator of what I think that's getting at.

But I didn't. I didn't get it from the words, that's all.

### P12: No opinion

Increase end user dependency. Yeah, yeah. If someone somewhat agree, I think that we could see, you know, shifts about that socially.

### P13: Somewhat agree

Yeah, I I I somewhat agree. I mean with the number of days, Charles, alright.

And this is a good example of some in many ways we're already there.

Charles: Yes, I suppose so, yes. So you think the improvements will be, we'll just do it better, not that we won't rely on, not that we'll get more reliant on it. We'll get the same amount reliant on it and it'll just get better.

But it'll just take different forms. Yeah, exactly.

### P14: Strongly agree

### P15: No opinion

I would consider putting this after point 6 - as 3, 6 and 5 are all about human interactions with CNI software

### P16: Strongly agree

### P17: Somewhat agree

And end user dependency was a. What was the reservation on that one?

Yeah. So I think we're definitely, I mean.

I mean, we're doing it ourselves. We're more dependent on technology to give us informed decisions. We're using Data, Data's being pushed as a new well. Data Data's always been dated, Data's always been used as a point in reflection and A and a datum to reflect on where we are and what we're doing and what's the deviation type thing. And now we're making more sense of it and we have technology that supports that.

Understanding a lot more from a business benefit, it's it's a it's a given. I think you know we we will do and things like generative AI will support that clause. I think so, yeah.

### P18: Strongly agree

### P19: Somewhat agree

### P20: Strongly agree

### P21: Strongly agree

### P22: Somewhat agree

### P23: Strongly agree

### P24: Strongly agree

## Question: System operators working through software, not directly

**Description**: By 2040 humans’ participation in CNI processes will increasingly be through complex software systems rather than directly with hardware or simple software controls.

Totals

No Opinion: 2

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 11

Strongly agree: 7

### P3: Somewhat agree

It's a little bit out of my side my wheelhouse. I have a strong opinion on it really, I hope not.

Yeah, yeah, yeah. I mean, you can sort of see it coming. I mean, what are they just to sort of maybe just a little nugget that.

And 16 networks. So the kind of future communications. And he was sort of talking about how there there is this real this real potential, OK. One of the things that you were talking about the motivation for 6G right in the US.

One of the motivations for 6G in the US this is sort of very informal, I guess, and you'd have to sort of. I'm not sure how useful it is to be able publishable, but one of the motivations for the US to move to 6G is because.

The patents.

That relevant for 5G.

Yeah, I'm not us owned the Chinese.

Right. So there's a there's a kind of a push to almost skip 5G because the ownership of the intellectual property for 5G technologies in the US, right? So then the question then is going going to your point about this sort of separation, you know, will we in the future have like it was in 2G? Like if you remember, I don't if you remember many years ago 2G, you know the US had a different.

Yeah, yeah. Different sort of.

Yeah, exactly. Yeah. So we have like GSM or something like this in in Europe and everything else. And in the US, they had a different standard. So there's a potential for that kind of.

You know, because of political and and sort of commercial reasons for the thing to diverge, but.

### P4: Somewhat disagree

Yeah, because because people are already working through software in, in, in indirectly. So it's the umm again I'm.

Maybe, maybe fewer people, but but I think there's always a sense that you can never have.

They'll never be too few people.

This this could that there's quite a useful tale which may or may not again may be relevant. So in my previous no, not my previous life, the life before that, when I when I was doing work at the space industry, my colleague was telling me about the time he went to a symposium on cost savings in spacecraft operation. And there's a team from NASA they're talking about when they're observatory missions. And they said we had Mission Control team of 80 people and we got it down to 60 people.

And then there was the the group from Easter there, and they had a comparative mission and they said, well, we had four people and we got it down to two people part time. And we really I mean.

Any more than that, it's not lean and mean. It's skinny and \*\*\*\*\*\*, so it's. But ultimately you're never going to be able to completely remove people. So these things are not going to be completely automated. So anyway, the the point is, that's the reason I I said disagree rather than.

### P5: Strongly agree

OK, I'm I'm gonna say definitely more automation all the time.

Yeah, exactly. I think back at the matrix, do you know what the matrix movie is?

And they have a scene in there where NEO and the old guy's looking out over and he says I don't know how any of this works anymore. It's all machines.

### P6: Strongly agree

### P7: Somewhat agree

System operator's working through software, not, not directly.

But there are many, many analogue systems, especially where where safety systems are concerned and operators are very much relying on the sort of analogue analogue safety right systems tripping. If something happens and I don't, I don't think I think it's some sort of the safety critical sectors.

You know, 2040 is about 15 years away now, right?

Maybe, maybe the mentality might have changed, but I'm not. I'm not.

You're not seeing it as a trend that.

I'm not 100% convinced. Yes, there is strong strong pressures to.

### P8: Strongly agree

Yeah. I mean, how can I disagree with it? Do you know what I mean? So that we are going there? Don't we are people are are divided on this and the software engineers. So do they know something that I don't?

Only weather, only weather. Actually, it's already mainly through software, so some people pointed that out and and yes the software will be more complex, but maybe it's already the case, was the sort of thing that's saying, but you know in, in your, in in transport world though at the moment there's awful lot that is not through software. So maybe that's yeah, yeah.

Yeah. From that angle, I would say yes, like an obviously that you know because I I came to transport from from.

A defence, so I can't talk. And there were a lot of reasons for that. And one thing that that shocked me was how transport was behind, how they was was behind in terms of software and everything. So they are quick change up, aren't they? So yeah. So for the thing of the.

### P9: Strongly agree

### P10: Somewhat agree

Rather than directly again, yeah, this is my my sort of my, my sense that that, that, that people in this sector really do value that the humans in the loop and.

In a sense, the this is. This is my sort of anticipation. These are my anticipatory assumptions. So the the acceleration of the, of the kind of the of, of the gpts and the kind of transformer platforms that is actually making people more hesitant. We know how error prone, we know how.

And it likes to hallucinate. We know how bad it is at maths, right? We also, there's also the issue of explainability with a lot of those issues and CNI of course that's that's absolutely essential. So are in a sense I think the the uncertainty around those innovations will particularly as we're looking at on this time time horizon, I don't think that's going to I think in sense people might be more you know more sceptical if we hadn't had the tap TPT revolution.

Then then that line must have moved in a different direction and faster, but that that's that's my thinking there.

### P11: Strongly agree

### P12: Somewhat agree

### P13: Strongly agree

### P14: Somewhat agree

### P15: No opinion

I would consider putting this next to point 3 as they seem related?

### P16: Strongly agree

### P17: Somewhat agree

somewhat agree on the system operators working through software

It's it. It will move towards that as as new blood gets into the to the CNI sectors, but because they've they've grown up with you know the the new generations getting into that field will have grown up with more technology than we did when we were starting out. So that's the differential I think there.

### P18: Somewhat agree

They're the S and a lot of this was. Yeah. And it's happening now. So. Yeah. So so when. Yeah. Yeah.

### P19: Somewhat disagree

### P20: Somewhat agree

Again, I probably think it will be a combination of.

Humans are machines as human machine teaming thing, and I think we're gonna completely.

And create.

Digital twins and virtual virtualized systems. I think that there'll be some still practical direct contact.

### P21: No opinion

No. How they how they typically work. I mean, my assumption would probably be yes, but I wasn't too sure.

I think there's also, I think in a lot of the cyber risk context that I move around in, I think there's a lot of awareness of some of these things and that some things aren't digitalized or aren't sort of interconnected and so on. So that's why sometimes I wasn't 100% sure with my opinions because there's an element of I tend to talk to the people who are were taking counter.

So they wouldn't tell me that everything will be digitalized and everything will be software, because they're exactly trying to avoid these things.

### P22: Somewhat agree

Then I think I achieve and it increase in digitisation and decentralisation. Yes, all sorts of clusters together, but the context is software is big, it's important, it dominates the reliability picture and complexity and interconnectivity drives the agenda.

### P23: Somewhat agree

### P24: Somewhat agree

Not the one about system operators working to software, not directly.

So the fact that.

I wouldn't.

Agree, and I don't think the proper pathway is just letting software systems run themselves, but.

There's there's a need of human participation, so I don't think it's gonna be like entirely automated.

## Question: Changing geopolitical context

**Description**: Towards 2040, two major trends will affect CNI software:

a. Segregation of the internet into separate blocs with differing values and standards.

b. Climate change and green energy movements driving digitisation and automation to mitigate harms.

Totals

No Opinion: 4

Strongly disagree: 0

Somewhat disagree: 5

Somewhat agree: 10

Strongly agree: 3

### P3: No opinion

### P4: Somewhat disagree

Yeah, I I don't think I personally mean I I mean this perhaps might not be my ear and it might be me over applying Occam's razor but.

I mean, geopolitics is from a defence perspective, geopolitics is having an impact, but it's having an impact now.

But I think the values and standards.

Are they fundamentally changing and you know, even if?

All of these countries had values comparative with the West. They're still gonna be state, state, nation interest in things.

I don't see that they would be any substantive change.

### P5: No opinion

### P6: Strongly agree

### P7: Somewhat agree

What? What? What do you have in mind when you say this? When you say Dr CNI to implement changes to mitigate harm. So what? What sort of changes do you have in mind?

Personally, I don't know. I'm thinking in the energy sector. For example, all of this move towards local generation of photovoltaic.

And wind and whatever else.

So in the energy sector, that's really important.

Automation. There are sort of cutting down on energy uses in the other sectors, I suppose.

Yeah, lots of lots of stuff happening there.

I'm.

Yeah, I'll say I'll, I'll say I agree. But as you say it's it's it's a busy question. I mean you could you could sort of focus on on different parts of it.

But definitely you know this side of things.

Different distributed energy generation through through distributed sources and all that it's already happening.

Yes, there is. There is a number scale, so yeah.

You see, and I well telecom's parts of telecoms is already.

### P8: Somewhat agree

Come in and we drive to implement changes to it will definitely for the second-half, you know it giraffes you need to implement.

I'm not sure about the segregational Internet into separate blocks with different beliefs and standards. I'm not sure about the whole that basically is a combined. Do I miss unsay anything here? Do you want to?

To be honest.

That one because I know that I provided some requirements around the climate change and the green mammoth around maintenance activities for infrastructure. So the UCCNI that is what I think of infrastructure. So there are changes that we are doing to mitigate harms because we're providing requirements. So from that angle, I would agree because I know that already that it teaches hip already.

At least, like in theory or in terms of planning for future to an extent the second-half.

I can't not disagree because we are doing it. You know what I mean? So, like, well, I'm sorry. It is driving. So it is not we driving it is driving right now. So you know but the but the first one I am not sure. So I just say somehow OK so for the reason.

### P9: Somewhat agree

Yes, I think the I might actually I put some specific comments on in the in the box below that relates to some of these, but in this one for instance, I I think the the information level that the Internet's already balkanized with different values and standards now the the telecommunications level.

Is still working to the same set of global standards because it behoves everyone to be able to interconnect to the same things. I know there are moves that the ITU for the Chinese to change some of that, but generally speaking it's at the moment it's still the same protocols over the same cables.

That still benefits everyone. We don't have risky net versus US net. We haven't got the Cold War blocks. But on top of that, in the information layer, your experience of the Internet as a Russian would be completely different from your experience of it as an Anglo American. Your experience as Chinese or as an Indian or actually as a German for a Portuguese speaker, those are there are very, very different norms and very different information sets that are available. So I think the Balkanization element is kind of we're already dealing with that. I don't think that's going to be so much of a problem.

That's interesting. So, so not a technical, not a yes, not a communication balkanism balkanization, but but an existing information one. Yes. Yeah. OK.

Do I think climate change and green energy movements will drive CNI to implement changes to get harms? I think it's already doing that. I think the back pressure of the financialisation is what we're really driving against there, not not the technology. All the people working in, all the people working in C and I utilities wanted to make those changes.

### P10: Strongly agree

### P11: No opinion

I'm changing geopolitical climate.

This has been going on for 20 years or so.

There's been a a schism in the world and I haven't kept up to date with it lately. Between China, Russia and some other countries that that, that believe that it's.

Responsibility as governing organisations as the as the the secret. You know, the Communist Party of China, for example, their responsibility to protect their people from bad things, and that includes bad stuff on the Internet and therefore they need control of the Internet. They need control for a variety of reasons and and therefore they have a completely different perspective to the West Coast, California type.

Which I think is entirely amoral. It's, you know, we are the network provider, we are not responsible for content kind of nonsensical argument, but what I'm really saying is.

It was the towards 2040. I didn't get really that there will be a segregation. I mean they've been trying to do it for years, different values, different standards, yes. And then the second sentence. I didn't understand how that fitted with the first one.

So if one. So what you're saying is it's more a continuing segregation of the Internet.

Yes. Yeah. And it's nothing to do with the CNI as such, except in the sense that this is part of the CNI.

Suppose I would say that the Internet and other aspects of the CNI will become may become increasingly polarised.

If the world becomes geopolitically more polarised or it reflects the geopolitical polarisation of the world.

### P12: Somewhat agree

### P13: Somewhat agree

Yeah. So I I kind of agree on the separation of the Internet.

I I can see that happening.

I mean climate change and green they they should drive.

That, but I'm not. I'm still. I'm still not. I'm still not convinced that the political wills will act on climate change is actually there. So.

### P14: Somewhat agree

Probably I just somewhat agree not, but simply because changing pillow could your political context is with us the whole darn time.

So it's not that it's not a significant factor, but what I want to regard it as particularly relevant to the period when we're getting to 2040.

No, it's relevant now. You know the world has been dividing into different blocks for centuries.

### P15: No opinion

And to adapt to the risks arising

### P16: Strongly agree

### P17: Somewhat disagree

Changing geopolitical context, apologies for this is really three questions or at least two.

And you disagree.

Yeah, I don't think there's gonna be a a segregation of like the Internet into sort of separation, you know, for like, you know, having private spaces for like C and I, connectivity and general Internet or something that that's kind of how I interpreted the the question.

So I don't think that's going to change and even with like promises about, you know what Web N three was going to be about, which is a new, which was a new decentralised Internet which is happening. But I don't think people realise the benefits and the adoption and the adoption. So I don't think the segregation aspect is going to come in anytime soon, to be fair.

And climate change and green energy movements.

I think there's gonna be more of a reliance in and there's gonna be an increase in OT infrastructure because you know, all of a sudden we're like, OK, we need, we need more distributed systems like renewables and so forth to support greener energy environments. And obviously that has to be controlled and control of that will become CNI. So there will be an increased landscape in that area. But I still think.

You know the the geopolitical aspects.

Might have an impact on that as such.

### P18: Somewhat agree

OK, climate change. And once we'll drive.

So the first one I agree with. Yeah, a second one.

Climate change and energy green energy movements will drive C and I to implement changes to mitigate.

Yeah, OK. Yeah, I can see that happening.

We're seeing that now, aren't we that?

So the the use of solar panels and stuff like that, which has been driven by climate change, ultimately you know, but maybe cost, but cost of energy is associated with climate change in the big picture, so and that's that's moving.

She's good to drive. See you tonight. Changes and and that's through, resulting in a diverse, dispersed grid. You know, generation.

And so there will need to be changes implemented to kind of make the grid or keep the grid resilient. Yeah. So I agree with both of those. Yeah.

### P19: Somewhat disagree

### P20: Somewhat agree

I mean I'm, I guess I'm concerned about the location thing, but I'm not, like, totally sold the little, the little happen. I think that there are incentives to keep it, you know, free and open. But I think that's probably the the direction of movement. And yeah, sure. Climate change in green energy movements. I think that they will drive and implement standards but.

I'm not entirely convinced that that's the thing that's going to guarantee that there's, you know, the the potential for harms is completely mitigated in these sectors. I think it's a factor. It's a variable, but I don't think it's the be all and end all. I think it will rely on other things like, you know, government regulation, corporate responsibility and so on and so forth. So I I'll only put somewhat for that as well.

### P21: Somewhat disagree

For me was the segregation of the Internet just because I think that's been predicted for the last 20 years.

Ah, and it still hasn't happened. That's that's a very interesting observation, OK.

And it still hasn't happened to that extent and we've talked about these things that are like my my original background is Internet governance and sort of UN processes and that kind of thing. And we've talked about the balkanization of the Internet. And so all that for so long, and it hasn't happened. I don't.

Yeah, I'm just sceptical that we will happen by 2014.

### P22: Somewhat agree

### P23: Somewhat agree

### P24: Somewhat disagree

## Question: New CNI

**Description**: Towards 2040, increasing digitisation will lead to aspects of the internet themselves becoming critical infrastructure.

Totals

No Opinion: 2

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 6

Strongly agree: 12

### P3: Strongly agree

### P4: Somewhat agree

### P5: Strongly agree

Fully expects to the Internet themselves becoming critical infrastructure. Yeah, we're already seeing this. We're seeing more and more movement to the cloud all the time.

### P6: Strongly agree

### P7: Strongly agree

### P8: No opinion

### P9: Strongly agree

### P10: Strongly agree

### P11: Strongly agree

### P12: Strongly agree

Decision digitization themselves be Oh yeah, strongly I go. We already live in that world. AI open doors to automation. Yeah.

### P13: Strongly agree

### P14: Somewhat agree

So because again, I just don't know how quickly it's gonna happen and it that's just based on lack of clear knowledge or understanding of the issues.

I can understand that that is going to happen, but I can't say I strongly agree 'cause I don't know the time scales.

And the scope or the scale?

### P15: No opinion

If it isn’t in practice CNI already - communications IS already a CNI sector and internet related infrastructure falls under that.

### P16: Somewhat agree

Yeah, I don't know why I actually I didn't go. We strongly agree, but.

I think that.

You've almost turned it round. You've said critical infrastructure will.

Yes, yes, I'll be connected to the Internet. Yeah. Yes. So, yeah, so it. Yeah.

### P17: Somewhat disagree

And you disagree with new CNI?

I think so. I know like my thought process was around this was, you know will we are and probably will move more towards digital twin based systems for like monitoring and modelling and and all kinds of features and so forth. So that is very much a sort of OT to Internet to cloud type aspect and that will increase. So there is an increase in digitalization in that front for example but.

I don't necessarily think it will become.

Classified as being CNI as such, because I almost feel like there there has to be a threshold of what what gets classified and what doesn't. And if you if you decide to classify too much I think.

You just you start to kind of fraud the industry a little bit as much as I want it to. Funnily enough I I just don't think it will, it will benefit this, it won't work this from a business perspective, I don't think.

Mm hmm, so this is likely to be more for information than control. People won't. Yeah. Yeah. OK.

Right. Yeah, yeah.

### P18: Strongly agree

### P19: Somewhat disagree

and I I remember going to our

Conference my old friend here in steroids in San Francisco.

I was on and he was getting some case tutorial that I was on the panel here.

Which is about Was to tell

Was a big event.

There was a chapter from the White House talking about the the 10 most.

Important National infrastructures 1 of them

Unbelievable

This is just how this is not that

and if I spoke to the chat box that it wasn't he who had produced the list

that people collected and the internet people think

the internet. What yeah, yeah.

And unfortunately So that that's why I put this 1 first and then these other ones.

### P20: Strongly agree

I would say that that's already the case. I think that they're already countries that treat Internet as critical infrastructure.

The only remarkable thing is that Britain and America don't. Yes, yeah.

I thought the US does now. Homeland Security doesn't provide, I think it. I think it covers Internet service providers and stuff.

The Homeland Security definition of CNI.

Don't know whether the I wouldn't be able to say either way confidently about the UK either.

It does. It's hidden under communications, but whether whether communications is interpreted as including the Internet I haven't established yet, yeah.

### P21: Strongly agree

### P22: Somewhat agree

I think new she and I digitalisations will lead to aspects of the Internet themselves becoming critical infrastructure that's already there.

So yeah, that's interesting that you're trying to relate to a nuclear communications, energy and health sector as well. Nuclear historic reasons is going to change radically. You're talking to the old nuclear sector with these big old legacy system. They're going to be phased out in the next 10 years. The nuclear industry is going to be small reactors, and they're going to be much more likely they're going to be much more like the communications, energy and health sectors.

And if you go by the the sort of the nuclear industry as it is now, according to my friends who are who were in it and occasionally called back as consultants, most of the stuff in the nuclear industry is now legacy. It was purpose built and nobody knows how to maintain it. And that's an important part of its on reliability.

But hopefully they'll be phased out before it all blows up.

And it's a sort of separate discussion because in the communications, energy and health sectors, what you've got is legacy systems plus a lot of in inbuilt stuff, a lot of in source stuff. You know, components that are built in. And so there's a lot of instability around the connection between the legacy stuff and the new components because they've all got different design assumption and.

So that came out in our interviews that that's a real source of problem.

But what xxx is very clear about is that when she looks at the resilience of the infrastructure.

Outsourcing outsources. Actually, get rid of legacy software a lot faster than anyone else.

### P23: Somewhat agree

### P24: Somewhat agree

Do you do new CNI?

Will lead to aspects of the Internet themselves becoming critical infrastructure.

Yeah, somewhat. But I think it already is.

Critical like the big the big.

I don't know like family and compass is already things of.

Digital tools, so it's already critical. I don't know. In terms of telecoms and energy.

## Question: Artificial intelligence

**Description**: Towards 2040, advances in Artificial Intelligence (AI) will open doors to increased and improved automation, situational awareness, data sharing and interpretation, as well as the development of more efficient, and effective systems.

Totals

No Opinion: 2

Strongly disagree: 1

Somewhat disagree: 1

Somewhat agree: 10

Strongly agree: 8

### P3: Somewhat agree

### P4: Somewhat agree

### P5: No opinion

You know, I'm gonna keep it right where it's at. I don't know. There's there's there's a lot of desire for people conceptually that they want AI to do lots of stuff, however, actual.

AI in use that's positive. I I don't see it much today.

Yeah, but I think the trend is moving towards for sure. So I'm just gonna say I in the middle, I don't know.

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

So artificial intelligence. It's meant to be open doors to increase improved. Definitely. It's definitely.

Situation awareness is a very.

How shall I say, is a word that we achieved? We're very careful in, in human factors it means something. But I think I used that expression.

This sounds like one of the things that I will do every time in product registries and data change is very disruptive. Do you know what this has? One of my sentences here you copy it from me. Do you know what? I have an article. It. It has exactly like this.

Because I yeah, I can, I can ~~shave~~ share it if you want. It is something today around the trucks. Do you know what I mean? So basically is the trucks and have the maintenance using the robots and artificial intelligence for data collection to increase their own situation and awareness and automation. And they share the data with some other parties and they can interpret.

And efficient, effective if only you put safe in here, I will say I have written it. You're only missing the more safe, efficient, effective here. Oh, my God. This my side. This really good. Sorry. I got excited. Like so something that I kinda you know, I just signed. I signed right under it, right.

### P9: Somewhat agree

Yes, but not the transformer based architectures. This was my caveat on that just because there's a lot of talk going on about artificial intelligence at the moment and a lot of it's actually about GPT, the llms and so on. In the meantime, there's an entire other industry that's been going on really successfully. I saw a great quote from an academic recently, the ctas event in London 2 weeks ago, three weeks ago where somebody said we've just come out of an AI winter. Do you think another one's coming and he frowned and went.

AI winter. Oh, you think nothing's been going on and suddenly we get ChatGPT and everything's changed. So we've been working all the other forms of AI have been developing really, really powerfully. But they're all the ones you don't see because they're actually doing useful stuff and suddenly you get a chat bot that can paint pictures of horses riding doughnuts. And you think the world's changed? No, this is this is an evolutionary dead end from an AI perspective. This will only go so far. It's when it's integrating with the other systems. It's going to get interesting.

So I think yes, there is enormous potential for AI and ML to make a play a massive role in us dealing with more complex systems, more complex changes.

I think that's going to require us to have trust and confidence in the logic and working of our expert systems. That doesn't lend itself to a transformer based approach. I think that will revolutionise the way we engage data.

But in the context that this presented here, I think is much more. The other elements of AI. So it was more sort of flag to go, yes, but not llms.

### P10: Strongly agree

### P11: Somewhat agree

### P12: Somewhat agree

### P13: Somewhat agree

I I I I am somewhat sceptical about.

How far and how widespread the current hype around AI will actually pan out to? To be? AI has been here 2 times before.

And has failed to up to the high.

You just have to take the example of self driving cars for an example that we've been promised for many, many years.

And it's just too much of a complicated problem.

To solve doing things in the real world that are not contract constrained, they're an open world, not a closed world, and it becomes very difficult to deal with that. And I don't. Yes, maybe we'll get there, but I'm sort of kind of sceptical.

That it will be as widespread as many people object, so I do. I've got somewhat agree, but.

Yeah, absolutely.

### P14: Somewhat agree

But other than another thing there of course which is which is that I think features elsewhere in your set but AI also carries dangers as well as promises.

So it could be opening doors to this, that and the other, but in the process you could be letting in all sorts of demons.

So. So it's not necessarily the panacea?

### P15: No opinion

Also additional security risks with deep fakes etc

### P16: Strongly agree

### P17: Strongly disagree

Oh, and you strongly disagree in advances in AI.

Improving.

Systems generally.

That.

I'm I'm a big fan. I'm a big fan, as everyone most mostly is in technology with with Gen AI at the moment and forms of it, but I think.

My biggest bugbear at the moment is we don't get cybersecurity right. In fact, we're pretty, you know, part of my friends were pretty \*\*\*\* at it. So now people are jumping onto this. Jenna, I bandwagon, which has been around for a while. I feel like we're not. We're actually increasing the attack surface with AI integration or aspects of AI which people don't necessarily see because they see the benefit. They see the upfront benefit rather than the actual.

Kind of business case for it. So I do think artificial intelligence, intelligence.

Whilst it can improve and and I do, I do agree with what it's saying, but I actually think the implementation of it will actually provide far worse benefit than it will do good just because I think it's going to expand an attack surface on an attack surface that we don't do well on at the moment, and now we're adding a different layer on top of that. So yeah.

I like the concept. A bad benefit is worse than a worse than a moderate good

Yeah, absolutely. Absolutely.

### P18: Somewhat agree

Yeah. OK. I, well, I could go agree on that. Yeah, as well as developing the more efficient. Yeah. No. OK, I'll go agree on that.

### P19: Somewhat disagree

### P20: Strongly agree

Yeah. I mean, I think this is undoubtedly the case in relation to AI I think there's maybe small question marks around efficiency and effectiveness.

Some are they all going to be like that. Are they? You know? Are we going to have ineffective AI and inefficient AI? Probably as well. But, I mean, I think the general trend is pretty strongly towards improvements being made in those areas.

### P21: Strongly agree

### P22: Somewhat agree

### P23: Somewhat agree

### P24: Strongly agree

## Question: Quantum computing

**Description**: By 2040, quantum computing will be starting to support solutions to a set of optimisation and cryptographic problems for a few international companies and nation states.

Totals

No Opinion: 6

Strongly disagree: 0

Somewhat disagree: 9

Somewhat agree: 4

Strongly agree: 3

### P3: No opinion

### P4: Somewhat disagree

No, it's the. It's the I I think some of the.

I mean a lot, a lot, a lot of this is all really about what point interest is gonna wane. And are you gonna get, you know, looking at your hypes of expectation or hypes of whatever it is. And I think it's.

Quantum might be going down a little bit. I mean, we're putting money into quantum computing. So I mean it's I think there are certainly applications for it.

It's. I don't think it's matured to that extent though, and certainly cryptographic problems. Yeah, I think people. I think the the search for an alternative key distribution mechanism and key establishing messen are well underway. The symmetive cryptography problem can just be addressed by just doubling doubling the key size quantum computers.

So maybe if that was 20, maybe if that was 20-30, but I think no, no, I think even then.

Caviar. I don't. I don't really work that much. So I'm I'm more of an observer, more of an observer, seeing how it's things are doing at the moment so.

### P5: Somewhat disagree

### P6: Strongly agree

### P7: Strongly agree

Yeah. I mean, yeah, I I guess so again 242040 is.

It's not that far down the line but but yeah, I suppose we'll see. We will see developments there.

### P8: No opinion

### P9: Somewhat agree

Yeah. My challenge around the constant thing is I think we're everyone's sort of worrying at the moment that we're on the cusp of having first quantum computers built and and therefore that's going to be the rate limiting step. I've, I've absolutely confidence we're going to build quite big quantum computers in the very near future. The technology is now reached the point where it's scalable and it's just a case of get the investment and build the chambers and add the qubits.

So I'm confident that's going to happen. There's still only about 2020 or so quantum computing algorithms.

But have been calculated and if they're not relevant to the problem you've got, you don't have an advantage from quantum computing. So I think we need to do a lot more research into quantum mathematics and quantum computation rather than quantum computers in order to unlock that potential. So that's my that's my caveat there. And I'm less well cited on the development of that technology than I'd like to be. But my sense is that's actually going to be the rate limiting step we're going to have these fantastic machines and go great if you can make your problem look like Shaw got Shaw's algorithm, you're in.

### P10: Somewhat disagree

Notify I'm just, I mean I I know it's a thing, but I'm just not by 2040. I mean I I I will be shocked and surprised when it comes out in 20, you know, 2037 and everything is is is broke. But yeah, I'm I'm that's that's my that's my friend.

### P11: No opinion

Quantum computing.

Oh, I don't know. I just just felt like no report is complete without mentioning quantum.

Yeah, I think you also have to be careful to explain what you mean by quantum. Are you talking about?

The use of quantum techniques for secure communication and other activities. Or are you talking about the ability of a quantum computer with superposition to a break non quantum resistant encryption? Well, they're two completely separate things, and neither neither of them to me appear to have a lot to do with what we're discussing, except I suppose.

For older algorithms.

### P12: Somewhat disagree

Quantum computing optimization. Cryptographic problems. Yeah. I just don't think quantum computing. I think quantum communication and sensing, but not necessarily computing. I guess I somewhat.

Oh, quacking, sensing, you know, like, outfitting satellites with quantum sensors to be able to, like, see through walls and stuff like that.

### P13: Somewhat disagree

Incredibly powerful concepts in concept and concept, conceptually engineering wise.

Some really big challenges to overcome that I think are probably beyond us before 2014 in terms of getting a quantum key computer to achieve any kind of scale.

### P14: No opinion

With quantum I just not sure it's gonna be done by the 24. That statement is correct.

Quantum will start to Support Solutions, but I don't know if it's by 2040.

Everyone says they've wanted one of those things where people say it's it's too 25 years away or 10 years away, but then ten years later, it's still 10 years away.

Yes, that's right.

Quantum definitely, but just not by that date.

If you look at my comments here, I agree, but this will happen. We're not sure about the timescale.

### P15: No opinion

### P16: Somewhat disagree

Well yes, because I think that it's it's it's, it's still and not and not disagree in the sense that I'm against the statement disagree in the sense that I wouldn't formulate it as with such certainty. So it's for me it's still a major question mark and and the and the and the qualifying.

Time frame also was the reasons of by 2040.

Don't know really. So I I don't I'm. I'm not sure I can agree with that or even somewhat agree. I just.

Maybe a lot more sceptical about that. I don't. I I don't ignore the massive investments being made by certain countries, but I think it's like AI. You know, the idea of AI was formulated in the 1950s, so it's like we are 75 years later and we are starting to see.

The impact. So if if we apply the same kind of logic to quantum, maybe we're still like 50 years away from seeing.

So but. But of course AI will accelerating and so we don't so so.

I I feel I see a lot of hype.

And and and still a lot to entangle with AI. So quantum, I don't know, maybe we'll have disappeared from the surface of the earth before as a species before we get quantum, right.

### P17: Somewhat disagree

And you don't agree with quantum. You just don't think it's going to be there in time, is that?

No, I do think it will be around in that period of time. But like if I look at so like if I looked at quantum quantum grip cryptographic attacks and what it potentially can do. So if you look at the ones that exist today and I'm going, I guess I'm going on prehistoric attacks, which is things like heart bleed and.

A couple of others which were to do with the cryptographic arrangements for confidentiality of traffic on the Internet and stuff, and.

Even they are quite difficult to pull off, so I really think that actually if the if the question was worded can quantum computing combined with AI?

Provide more problems than I would say yes, but quantum on its own, I'd probably say it will. It will provide something, but I don't think it will. It will be as as as negative as it is its intended to if that makes sense. You know so.

### P18: Somewhat agree

Yeah. So, I mean it's there now.

In small bits.

So that's obviously it's less less advanced than artificial intelligence. I just, I just think, yeah, I couldn't commit strongly to that because of the difficulties in making good quantum system robust and kind of usable at the moment. So yeah, and there are problems with it.

So I just think it's a technology maturity issue is the reason why I've got completely for that?

### P19: Somewhat disagree

But but the content makes no sense to them at all this contest.

Yes. I I've been tracking people working on content fields for some years.

I mean 24 is actually possibly a little early.

So that's what everybody well.

People have been working.

There's a

Vienna they all technology that I know course and they've been working

on quite a few years.

You can't demonstrate much.

They also can't really explain very well.

What they do. I find the the application of it.

Previous Actually in this context and almost to be in the business of this optimistic.

You have to be very optimistic actually to to think some useful come up.

Just means A lot more computing power is coming up when when they realize the potential

that we already have faster that sort of competing for and in that way that's quite

important and so forth they are.

The abilities and and a lot for it.

I I find it.

It's not exactly dishonest.

But I I find it.

Not not. Players of some people we talk about AI Department knowledge and not admitting

that really a lot of what's going on is out in Canada.

Yes, I think it's quite convenient to to regard AI as something that has got.

More potential than it probably does.

There's a there was something I saw in the newspaper that weekend.

I Thought that very very rough, correct?

Someone Could remember me as well.

Someone was someone fairly.

Knowledgeable which commenting on the saying that really we have to overcome.

Yeah, which

Stuck in the jail including stuff that economics that just depression as well the

economics of there. No, no, no, sorry.

No, no.

Sometimes

### P20: Strongly agree

So

### P21: No opinion

### P22: Somewhat agree

### P23: Somewhat disagree

No, I mean.

I guess so. I just last week I got back in focus on this 'cause I I went to University of Amsterdam and to give a talk about it and to their quantum group. And I I think one of the problems is that, you know, back in 2017 people were writing articles that saying there will be commercial quantum computers in five years. And so to get ready for this talk, I went out and I looked at the literature and now.

I think there's three different companies again.

Five years, but the when they use the the five years, they don't provide any specificity of why it's five years. It's just like, you know, five years that sounds right.

### P24: Somewhat agree

## Question: Off-the-shelf hardware and software

**Description**: Towards 2040, CNI systems will increasingly be made from off-the-shelf hardware and software components.

Totals

No Opinion: 3

Strongly disagree: 1

Somewhat disagree: 3

Somewhat agree: 8

Strongly agree: 7

### P3: Strongly agree

### P4: Somewhat disagree

Have you ever worked for the real time operating system? Would you consider if you looked at the X-rays? Would you call that cots?

And and you have worked with vizviek you have worked with Vxworks before.

Oh, sorry, no, I haven't actually, so I don't. I don't know who produces it. Come to think of it.

Wind driven wind driven, yeah.

When driven well, yes it is. It is commercial in the sense that it's not designed for any specific purpose. It's it's similar to Microsoft Windows, but for a different. Yeah, yes.

Yeah, yeah, yeah, absolutely.

Yeah. So, but it's not, it's certainly, I mean Microsoft Windows, you can get the C to your download it and run with it without the instructions, there is no way, no. No way, no how you were doing that with, with, with, with, with the real time operating system.

Even if bits of it are containerized. So.

I think there are bits of the national infrastructure are going to be comparatively more, more expensive than the sort of stuff you would download from an App Store.

Simply because they've got higher demands and and and a higher expectations and these sort.

Well, it's. I mean, my definition of off the shelf is you buy something and use it.

I think it's probably more bespoke. I mean it. I think it's more bespoke than. I mean, you're not gonna put that. I mean, it's not like getting a suit and sticking it on. I mean, it's in some cases that's fine. But the sort of C and I you want to, you're going to want to do a bit of work with it before you actually.

Before you actually it. So it's more like buying ingredients from from a supermarket and you know.

Would you consider the different classes of software? So with one hand you've got off the shelf. I mean, at some, I mean, nobody's writing. No one is writing.

Everything completely from scratch, because you've got, you're not, you've you've got pre-existing hardware and pre-existing board support packages and pre-existing firmware. You're probably going to take an operating system, be this and it's be this embedded or or or desktop.

So these these individual things are not off the shelf, they are, they are they they expect a certain amount amount of of cost customization.

Cherry BSD, for example. That's certainly not off off the shelf. I mean, you can obtain it's it's downloadable, but you know you're not just going to start using it.

You need to do sufficient amount of bespoke bespoke work and I think that probably goes.

For most software that will work in a in a in a C in A/C in that context on stuff that really matters, that regulators would actually care about.

### P5: Strongly agree

### P6: Strongly agree

### P7: Strongly agree

Yeah, they all they already are. I'm looking at the off the shelf. Yes, they already are. And there is.

You know, there is acni vendors that trying to to promote the sort of as a service.

Paradigm. So, you know, offer services in software on top of relatively commoditized.

Hardware.

It commoditize industrial hardware, not not not the kind of hardware we use. We use incorporate environments, yes. But I was speaking to.

Why was I speaking to Rockwell recently and they were they were saying they were saying exactly these, that they're they're trying to sell as much as possible, the sort of FAZ itself off the shelf and as a service.

Paradigm. But of course you know the signs of contracts that they might they might get into with with one of CNI or A/C and I operators means that you know they can, they can do anything essentially.

### P8: Somewhat agree

Thank you. Off the shelf.

To be honest.

If they do that, we have a lot of problems, but I do agree that will happen and we will have a lot of problems. Do you know what does it mean as a human factor person off the shelf? Hardware and software are one of our biggest problems because the users don't come in one box and then they are changing all the time. So we have to deal with like an aftermath of mitigation of the state because of the shaft, their heart and expensive to redesign.

So this is quite problematic. I will say yes and very problematic because obviously we prefer them to be designed from scratch. So I would quite like an agree with a lot of things. Isis strongly agree I signed right under it. OK. So I just put this one further, baby, that's good. Thank you. Yes. So they're going to make it more and more. It's going to be tough in the future and they're going to be more problems like because 2014 not that far away, you know, just around the corner.

### P9: Somewhat disagree

I I reversed the logic a little bit on the question.

And.

I think systems that we know before we start building them are going to be critical national infrastructure. We will ruggedize the off, the shelf components. I think we will, we will go in knowing this is going to be attacked and if it fails it's going to be bad for lots of people. Therefore I'm not nipping down to RadioShack and buying a server. Yeah, on the other hand, I think we're going to build a lot of systems out of off the shelf components and then suddenly go oh heck.

30% of my economy now depends on all those bits from RadioShack working. I wish I'd built it properly in the 1st place, so I think we to take an example. I wish you back to the llms. There's an entire industry now building commercially facing tools and taking contracts for tools that are built to run on top of existing large language models that are built by big providers.

And then those big providers keep changing the underlying Model 1. They're upgrading them regularly, which actually eats their lunch because the new general version does all the special stuff that you've just built on top, but also.

Or have it ever been really important?

And it's now that's now baked deep into the fabric of it. And it's a fundamental weakness those I think we are going to see. So I think we're going to see commercial off the shelf risk emerging in systems that were never intended to be CNI, but become CNI. Things that we know are going to be CNI like these small modular reactors, they are going to be stupidly expensive because we're going to build them to the right standards to start with and probably over engineered to start with, yeah.

### P10: Somewhat agree

### P11: Strongly agree

### P12: Somewhat agree

Yeah. I mean, I think like almost everything is and has always been plugging together stuff that already exists. But often I think it's the loo that you write in house that actually matters, you know? Yeah

### P13: Strongly agree

### P14: No opinion

### P15: No opinion

### P16: Strongly agree

### P17: Somewhat agree

### P18: Somewhat agree

Yes, I think somewhat agree. But I also think.

Because of the challenges with with diversity or lack of diversity, then there may be some stuff that isn't available. That's like purpose built.

So yeah, I I agree that increasingly it will be off the shelf, but it's not. It won't be completely off the shelf. I think there will be some, some bespoke stuff as well.

I mean you you cover different.

Yeah. And you're and you're including defence in C and I aren't you? Yeah. A defence infrastructure. Yeah. So that's one of the drivers from the in the defence sector was to because of the security implications of things like, you know, of of computer based systems, then they've gone. They've done their own thing to make sure that the baddies don't know what goes on in there. So it's that's driving stuff to not be commercial off the shelf to be bespoke.

### P19: Somewhat disagree

### P20: Strongly disagree

I don't think that they're entirely in using entirely bespoke systems in all of their operations, so I mean, especially when you think about health, you know, if you include health sector and things, they're using crappy Windows software. So I mean.

### P21: No opinion

### P22: Somewhat agree

I would also think that off the shelf hardware and software #11 is already there.

### P23: Somewhat agree

### P24: Somewhat agree

# RISKS

**Description:** General comments about risks

<Files\\P11R2> - § 8 references coded [4.36% Coverage]

I found it hard and I was really thinking I'd prefer to drag these onto A2 dimensional.

Impact likelihood.

And the yeah, it's because you see that the where is it now?

Some of some of them, like common mode failures.

I I think are highly likely and and they smear across a series of, you know, impacts.

Where is the I'm looking for.

You got EMP somewhere in there. I can't find it anyway.

I and I I think it is a lesson from the Ukraine conflict. It is that the way you harm your opponent is by destroying their critical infrastructure.

And the Russians did that to the Ukrainians before the tensions became all out war.

And Ukrainians are now trying to damage as much of the Russian oil generation as possible, and and their electrical supply.

I don't see that anywhere in here. I don't see the the the critical infrastructure will become a target and it won't be long before non state actors recognise this as well.

We all live in the you have different match will look to each other. We live in the real world. Let us let us mutually calibrate what it means. If people do this kind of thing and let's let's agree what is not acceptable like we're not going to attack each other's hospitals or are we so.

I think actually it was question 11 where I thought that would have been better on a on a likelihood impact grid.

Yeah, I'll think about it.

Yes, because some of them, I think that that this is the point where I saw electromagnetic storm.

And such like as being more like a Black Swan event.

Whereas some of the others I think are quite likely, well, they're sort of almost likelihood of 1.

Yes, exactly.

<Files\\P14R2> - § 1 reference coded [0.62% Coverage]

So is that a credible threat set of threats? Yes, in some cases, I think they're credible threats now.

Which is my concern with quite a few of them in this list is actually, I think they're present now. I don't think they're about the future.

<Files\\P15 Comments extracted> - § 1 reference coded [1.77% Coverage]

Might be useful to break these down into malicious and non-malicious risks.

Also I would suggest highlighting whether these are new risks (rarely identified in risk registers - many of them are already acknowledged in emergency plans and mitigation actions) or whether they are known existing risks, but the impact or scale or exact nature of the risk is changing in some way.

<Files\\P16R2> - § 4 references coded [1.60% Coverage]

Already we're investing massively in very traditional things, so so that's a risk. So it's the unknown, unknown kind of risk that we should really pay attention to because the kind of conventional risk that enter into the well established.

Matrix risk matrix. You know we we understand them those risks.

To me, they're still kind of potentially.

Well, we didn't say catastrophic, but potentially very serious.

Right. Yeah. So so they may not be the ultimate, but they are still probably the most serious things we need to deal with. Yes. Yeah.

Yeah, because we're we're already investing billions of dollars in other types of risks.

That we understand better this one, you know kind of response.

<Files\\P22R2> - § 1 reference coded [1.34% Coverage]

So the the risks, I mean I thought that the ordering.

Maybe if it was sociotechnology technological problems.

First, our second cascading problems and 3rd failure from.

The other infrastructure, but that's a sort of cyclical thing because you're actually talking about, you're looking at the comms and energy structure and now you're saying the comms and energy structure might fail to deliver the comms and energy structure. But I'm not quite sure what that's about. But anyway I've got.

<Files\\P6R2> - § 5 references coded [9.91% Coverage]

For the, I think it was the third or fourth block. I don't know. I made a comment on there.

These there are then the list of prediction in 2014.

And here it's depends on. I made the comment that depends on what you mean. So if we enhanced in in the from the taking the position, if we proceed as we're doing it right now. So we just go on in a linear development, all of those risks will be definitely there of course. And that's I guess that's part of your work. If we now address this individual chapters and change.

Our way of way of.

Building systems and operating systems and using systems then of course.

The answer will be if we if we do it now. If we make now the right decisions and do our developments in the proper way, in an ecosystem, in a multi stakeholder ecosystem, then of course all of those issues will.

However, not for me it's difficult. However, what you're asking, I would say it will not happen because we have changed the way of system design, system development, system operation so that that's the only point depends on how you are seeing it, what you want to hear as an announcer.

And and there of course is also then the parity setting in there, because of course if we addressing all those fields, you're covering all of them, if just in some areas we prepare appropriate countermeasures or mechanisms in our multi stakeholder environment, then of course some of them will, there will be a big thread and some of them we will have under control. I would answer it that way, but that's a different way of asking.

If if we don't do anything, then all these forecasts will happen. If we stay on in the current way of what we're working in all areas, then this will happen. I think that's very important. That's from my point of view, a very dangerous situation. So we have to change. That's for me, the management and we have to change our way of how to build system, how to operate systems and how to use system, what kind of tools are we using to use the systems that human beings.

Are supported by appropriate tools at them. That's what we have to change, I believe.

Exactly. It goes immediately into a specially, I believe, especially when it's we're talking about digitalization in a very critical.

Part of our universe.

It's also changing, especially those which are building an operating system in terms of education and skill development.

So in a nutshell, what do my management summary with Pete to all your questions, if we still go on that we.

Do innovation that we think about it and then we start to write some lines of code and then we have at the end how the millions lines of code and then we try to protect it and to manage it. It's not feasible.

So that doesn't work. So exactly the system engineering the system of system.

Understanding with architecture interfaces where we can then do all the risk management and protection mechanism and start to understand the enormous complex system because we have again building blocks at the end which we can treat with. That's an important way of I think changing also in the head.

Of the people which are learning technology and the danger is from my point of view, it's already happening. So I think now since he is already and this will be more and more, we are starting to use, developers are starting to use libraries which are out there but it open source or call it it's there or now we have all these famous AI driven new mechanism development is already going. So it happens already. You cannot prevent it. Engineers are asking chat TTP please write 3 lines of code. It is there, it works.

So we are still again increasing the innovation cycle. That's good.

But of course, if I ask chat GDP write me 10 lines of code so it works. But what else is in it? What kind of side channels are in this code? It's and then we have 100 millions of these building blocks. It's done so this way of system engineering could not work. So that's for me the most critical point in the most important point of what it has to summary. When we talk about critical infrastructure.

Is on the definition what you had the beginning. The way of designing and building the system has to be changed fundamentally.

<Files\\P9R2> - § 12 references coded [6.53% Coverage]

I think I think running down is all of my all of my somewhat agrees.

Are a a somewhat because of this point I made that the way that these are expressed, I think I said it in the comments at the bottom.

If we accept this sort of four part model of agent based risk, I absolutely agree that the opportunity for these things to occur is increasing because of the trends outlined earlier.

Whether that means the risk is increasing entirely depends on all the other factors, and if you're asking me to judge if all the other factors are held still, is there an increased risk? I mean take that first one.

No, I I I don't. I think I think to my mind, what what really something I was really reading through it and and drawing together sort of what's the one thought that all of this brings together. As I say it comes back to that.

As ever, a conversation about risk, I think benefits from precision in what we're saying.

And I don't know what opportunity you have to leave that in or how it works with the intentions of the paper, but to my mind that that model of saying the more I can decompose the causes and impacts of risks, the more precisely I can talk about them.

Rather than sort of general themes, but with that in mind, those are my thoughts. And then there was that point around.

The you can't look at any of these things in isolation, so the increase, the need to drive the utilities in the UK through the energy transition will mean that they will all be changing. They will all have to be more integrated.

The we will have to change the way that we use them as well as the way that we provide them.

Yeah. So so for example, if we wanted to replace our sum of our methane distribution of energy with hydrogen distribution because we don't want the carbon going, we only want the hydrogen going through the network to make that much hydrogen, we'd have to double the amount of freshwater that the UK consumes every year because you have to hydrolize fresh water to get the hydrogen.

We don't have enough fresh water already and we want to go and add more, so there is some, there is some interplays there, if you if you want to look at water consumption, you have to think about wastewater.

Handling and treatment if you're looking at wastewater treatment, you're pushing air through those wastewater treatment plants. It's even better if that's oxygen, they last better, but you make the oxygen by hydrolyzing water and releasing hydrogen. So you've now got this quite potentially complicated interplay of producers and consumers, and that almost works better at a more modular, granular, distributed level than it does with big central distribution networks. We've also got the issue while we're doing all of that, 50% of well, actually, no, I'm producing 100% of the electricity I need this summer from my solar panels, but I'm only using half of it because.

So it's one of my To Do List items that I never get to is change my electrical provider. So with all of these things being connected and the consumption patterns changing, if we all shift to electric cars that changes everything as well.

We have the potential to break the overall system, so I think the complexity really matters and I think that's the integration piece that creates a new, let's call it a tax surface for problems that don't necessarily have to be bad guys attacking it could just be accident, but you create more systemic potential for cascading risks and so on.

But at the same time, you know that, so you'll start to manage them. But that means that there'll be other changes and what look back teaches us about the introduction of new technologies in, in the battle space is the enemy gets a vote in how that evolves. And likewise we as the operators of these systems, we get to vote in how they evolve as well. So I think the.

How we manage these risks is going to be a complex interplay of of how we express the the different things that are coming.

Yeah. There you go. So I think those, those two factors express exquisite expression of risk and recognise that nothing happens in isolation and the enemy gets a vote. And I think those two things give us a rich conversation around how this is likely to evolve.

## Question: Poor response to accidents or attacks

**Description**: Towards 2040, we shall see increasing failure to identify and respond to adverse events due to:

a. Poor human response due to lack of training or trust in bad quality data or obscure algorithms,

b. Additional malicious activity, or

c. Glitches in AI-based situational awareness and guidance.

Totals

No Opinion: 3

Strongly disagree: 0

Somewhat disagree: 6

Somewhat agree: 11

Strongly agree: 2

### P3: No opinion

Yeah, but then even then, with the sort of due to the lack of training or trust in so because of a lack of training.

I mean, I I I kinda think you know, if I look at it now.

I think we're sort of aware that human skills.

Is an issue right?

It's a challenge we don't have enough people with the right skills.

Will that lead to?

Ah yeah, I don't know. I mean, I mean the issue there is that we're talking about automation a lot, which.

I just it's a difficult one to unpack, really. I think that's the the issue I have with it. 'cause, there's so many factors.

That kind of contribute to.

My my general impression is, is that I think we're probably gonna get better at it.

You know, if we if we you know if we believe you know, we're going to get better at security automation.

Yeah, exactly. And you know, and then sort of trusting bad quality data, obscure algorithms. I mean, you know, we're doing a lot of work on kind of explainable AI. If we're thinking about AI itself.

You know, there's a lot of reasons, you know, I think there's a general awareness now perhaps for certain types of things that AI isn't necessarily it. And we can do some stuff with less obscure algorithms. You know, a lot.

Additional malicious activity.

Yeah. I mean, I think they will be, I don't know if it's additional or different malicious activity.

Will there be more product?

Yeah. Yeah. They said, yeah, the dividends of the dividends, evidence of that.

Yeah, exactly. Yeah.

Glitches in yeah, I mean.

So what do we see? I mean.

I think you know that that sort of piece around.

Malicious activity, additional malicious activity. You know that you can see there's not.

Direction towards development of new capabilities.

Will we ever see them used? Hopefully not 'cause. I I think you know there are sort of.

I don't know norms.

Like that sort of prevent that. I mean the the, I don't know if I talked to you about it last time about this, Charles, but there's this kind of the in the NCSE.

From this year or last year?

They talk about state aligned threat actors.

Yeah, yeah, yeah. And and I think they're possibly a worry in the sense that they're a little bit kind of less constrained.

Yeah, I don't know if I'm. I don't know if I'm saying anything very meaningful about this, why I had no opinion about it.

### P4: Somewhat disagree

Full response to accidents. To attack. We'll see an increasing failure to identify. Respond to. Yeah. I think this is the increasing bit as well. I mean, I think it's I think you'll still see failures.

I don't know if they'll be increasing because I mean at some points.

The right, I mean, look at privacy, for example.

You know, it was it was a bit, it was, you know, 20 years ago, it was a little bit of the Wild West. And in the US to some extent, it still is. I think GDPR came along. It didn't solve the problem, but it kind of normalised things and expectations a bit more and and and sooner or later if these if the market is is impacted, someone's going to step up and try and do something because it's in everyone's interest for the, for the market to be used to be sort of stable.

In terms of accidents and attacks.

I think accidents you're seeing changes in norms, changes around occupational health and attacks. You're seeing much better instant response and security operations.

So I I think these things will happen, but I don't think it will necessarily be. I don't think it will increase exponentially.

### P5: Somewhat agree

Yeah, I'm gonna say I somewhat agree that it's gonna be more difficult for humans.

In their response.

We find right now that a lot of people are not trained up as much as they should be, especially on technology.

And glitches in AI after they start getting more and more.

Into society. I think that'll be difficult as well. So I'm gonna say I somewhat agree with this.

That there will be a poor response.

Well, this is happening right now.

### P6: Strongly agree

### P7: Strongly agree

Yeah, it's an interesting way of putting it 'cause the the flip side of it is that attacks just become too sophisticated to have any sort of reasonable response in, in short time scales, right? It's not so much criticising the response, but.

Yeah, yeah. Poor poor responses means that someone doesn't do what they're supposed to do. Right. Which which? Which is not fair.

To some extent, if you see what I mean.

Yes, yes, there's another one. It's not. It's not so much additional malicious activity that somebody's actually sabotaging the response. It's that the attack is so sophisticated that no response is possible. Yes, yes.

### P8: Somewhat agree

Design I was a bad design is one of them.

So when you say about poor human response, if the I think if you talk about if the system is too cumbersome, too complicated for mutual response properly if it didn't take into account my limitations, again as a human, you know like now like I am, I AM 43. I told you my age. So now I am not as quite you know responsive as when I was 23, it is not my fault is it? So it is not because lack of training because you cannot always train.

The non operators because it could be just you know, someone who's need to job or just a member of public and so on. So the desire should take into account my age, my mood, my morning shift, my night shift and how busy I am my workload.

I see the human responsibility being blamed in here, so just about I'm in the pure human is not due to lack of training because you know what? You can't train for everything. You can't train for bad design. You can't. How should I say mitigate?

A space design through training. I've seen it many years ago in defence. I've seen it many years ago in highways. I keep seeing it in rail. It's like if you train the humans we can overcome the bad design. No bad design is bad design. Design proper to start with. So this is the tissue. The meaning, you know, I just made a T-shirt like this. Bed Design is a part of the problems. So I don't know how to answer this due to lack of training or trust in bed quality data. Again, you can't blame human training a trust.

Problem here is not training. The problem here is not the. I'm sorry it's not the trust because you're just putting it as if it's a trust.

Or the abstract algorithms could be a partially agree with it. The whole thing in terms of like addition, emissions activity, yes, and the glitches in AI based situation areas and go definitely. So one of them is I am half agreeing the other one is like somehow agree I don't know which one I should click.

Do you hear? Partially. Yeah. OK. OK. I don't know how to write. Here is the bed design. I don't know how to write.

So, OK. OK. Focus on bed design. Don't focus on humans. Human limitations are, you know, like, like you, you cannot programme me. I'm sorry. I'm a human. I wish you could. I would. I wish you could. I would go back to my 23 year old self. But even that may not have, because then I have all the other issues. But anyway, so we're talking about this one. The other thing is Please note down as well. Is as you know with yourself the attacks are getting more and more sophisticated because why are they engineers?

And designers not.

Hey, Kim, if you like into kind the human limitation, I'm gonna be 10 capabilities the hackers did. They are smart. So they are actually doing this on the other side. So this partially why the second one comes additionally malicious activity because they figured out ways by understanding human psychology interesting isn't it? Hacker. I spoke to like an extra curve when I was in the Cybersecurity conference in Europe in 2019. And he said that we are studying more psychology than engineers did.

The very smart people do you know. Anyway, so only if the engineers thought about this much. I guess you say if you can't think of it in that way. So. OK, so you're recording this. Don't use it. Like against me, OK?

### P9: Somewhat agree

Yeah. Can you just run the remind me of the four part?

Opportunity.

Capability and resilience.

Yes.

OK. So three of those are from the attacker point of view and the last is the defence, yes.

Well, it intentionally.

I know intent and capability are what the attackers choices are opportunity IE have you designed this thing to have an attack surface and resilience? So are the are the defensive positions yeah.

So when somebody says we're gonna see an increasing failure to identify and respond to adverse event due to poor human response, it's like only if we don't address and fix that.

Yeah. Yeah. So I think I think you know the the potential of a poor human response, what the potential of let me rephrase that in a way that I would like it the lack of training leads to a poor human response, meaning we see failures occur.

Continued lack of training will increase the the the rate of poor human response and therefore increase the potential which is, I would say, is a resilience question, reduce the resilience of the system because we would respond less well.

And that one, I might say, well, yes, the logic's right. But it all depends on the lack of training bit. Do we think there's going to be a lack of training? I mean the logic is right. But so I somewhat agree, but I'm not sure that they've got good evidence. There's going to be a lack of training.

Trust in bad quality data is do I think there's going to be increased trust in the bad quality of data? I'm not sure I actually agree with that because I think we're talking quite a lot about the risks of bad quality data. I hope we're kind of ahead of that.

And then obscure algorithms. Yes, there probably is, but again, the challenge to that is better training. So we know what we're dealing with. So it's quite a complicated causal link you've put in that simple statement. And I kind of accept the overall thesis that, yes, that set of logic is true if the initial predicate is true. So if we were to express that as saying.

There will be a lack of training.

Leading to all of these things happening then I can say yes. If there was a lack of training that would happen, do I think there's going to be a lack of training or not now I'm now I'm doing some forecasting now I'm thinking no, I don't think so. I think industry is going to be on top of training. So I think we might be OK and that's why I sort of somewhat agree. But I've got this itch in the back of my head that says if I ask that question in the right way, I would go. No, I think we're on top of that.

And I, you know, and glitches in AI based situation awareness and guidance.

Do I think that's going to happen? No, because I think people are actually being really quite careful about AI at the moment.

You know, particularly in these mission critical areas, there's quite a serious conversation about.

So the opportunity space has definitely increased. Do I think it leads to a higher risk? I think we might be addressing it. So there's so it's it's a nuanced response.

That's that's led by the question, if you like. I feel I feel a bit, I feel a bit like I've been led as a witness.

### P10: Somewhat agree

Yeah. Yeah, that for me, that's into the resilience kind of space and and kind of poor preparation and poor. And I just think we've got, you know, as as a nation we're we're not very good at this.

Exactly. And there's. Yeah, there's there's been some investment, but it's it's tiny and it's it around building a secure and resilient world out of ukri. And there are a few hubs there, but and I'm on the Advisory Board for for one of them, but it's not it's, you know, it's really not obvious what difference it could possibly make.

But so yeah, I think that poor response, we know that this is not this is not well. Well, well done. Yeah.

### P11: Somewhat agree

### P12: Somewhat agree

### P13: Somewhat agree

Increasing so I I agree, we'll see increasing failure to identify response to adverse events.

Well, I mean.

Let's see. So let me go back out. There's poor human response.

Edesto says, yeah, well, probably feeling slightly optimistic when I answered this question.

And not all doom and gloom.

I mean, all, all of those three things listed there could happen. As I've said, I would think well, optimism that maybe they won't, but she'll say.

### P14: No opinion

And there are quite a few. There are quite a few elements to it, so we shall see increasing failure to identify and respond to adverse events due to poor human response. Well, that's definitely there now.

### P15: No opinion

### P16: Somewhat disagree

So I think so. And for me the, the the big reveal was the pandemic.

Because massive disruption, global disruption to systems overnight and still.

Massive adaptation capacity. Massive creativity, demonstrated systems didn't collapse, although we shifted half of humanity online overnight. Almost.

So infrastructures remained functional, wasn't pleasant in the first few weeks but still worked. So so so to me.

The reason I I'm I'm I somewhat disagree, not strongly disagree is that we tend to underestimate the adaptive capacity of companies and systems and people.

And we discount that too much. And I think that we.

We we, we, we yeah, we underestimate all the resources that are being poured into cybersecurity and and it and resilience and we we are admiring the problem of attacks and systemic failure and we fail to consider seriously all the efforts of people and all the all the commitments of people who are ready to actually tackle and address those challenges.

So that's why I somewhat.

Disagree not strongly, but somewhat.

So so you've got poor response. Oh, despite the mild degree, you've got poor responses first.

Yeah, but that's poor responses to accidents or attacks. So that's the that in the sense that.

That is still a risk, very kind of.

Very real risk and we cannot depend so, so so the the.

The pre.

Answers were OK, like statistically speaking, what are the odds now? This answer is OK well, from a policy perspective, where should we focus first? So we already have established that statistically speaking.

Probably everything will work as intended or people will find the resources, but because of that I think that's number one priority number one risk that we don't.

So we'll find the resources, which is a good incentive to invest a lot more into that capacity to make sure that we we keep on raising the bar and we keep on equipping people with the right and and and we don't ignore that and we don't.

We, we we we don't ignore the investments that are needed to maintain that capacity. So that's that's my logic behind it.

So the the the the reason I'm I'm I'm ranking this one as #1 to give you a very concrete example we have no.

System to measure or to rank the quality of response to a past accident or cyber attack. So we never do a postmortem where we actually try to measure the quality of the response and try to so, so very limited research.

Into that you see.

Same with attacker technology. We have very few tools that enable us to say with authority you know how this democratisation of tools is impacting.

The the the frequency and the severity of attacks. So we we don't model those risks and therefore it's it's it's a big question mark for me. So that's why I wanted to.

To to I rank them first.

### P17: Somewhat agree

I sort of dragged the ones that I thought were in the top five. That was kind of my, my viewpoint.

So like. Yeah. So like, yeah, the the poor response to accidents and attacks quite often. It's not really so in some cases it is leverage to sort of help better an organisation. But I've seen in some cases where it doesn't collectively improve the industry like it's not knowledge isn't shared information in Intel is not shared. So that's quite quite a key one for me. Obviously the human vector, the human fact. Sorry. The human factor is still quite a key one it's still quite a high one.

### P18: Somewhat disagree

It's a word failure in it. Yes, all those things are gonna happen. Yeah, but but my argument is that if you design it properly, it won't result in failure.

So there will be an increased human response. There will be additional malicious activity, there will be glitches in AI, but it's the fact that you're saying it's resulting in failure. I disagree with because if things are designed properly, you can avoid the failure.

Yep, and you if if it's if it's, if it is critical national infrastructure, then it needs to be protected, it needs to maintain resilience. So you can't accept those things that have going to happen without putting the right, the right mitigations in place.

So

### P19: Somewhat disagree

### P20: Somewhat agree

### P21: Somewhat agree

That I think that some people actually respond quite well to accidents and attacks, particularly large companies, and sort of those that are relatively trained in that context. And a lot of CNI is with quite mature large companies.

I mean, I don't think they're flawless at it, but I. So I felt, yeah, I somewhat agreed with that. Like, yes, there's still a lot of poor responses, but at the same time, I think it would be, would be too dismissive to say that this is the main risk that people are in, particularly in, like, large infrastructure companies are a useless responding to this. Actually, they're quite crisis trained.

I

### P22: Somewhat agree

### P23: Somewhat disagree

So with machine learning could be defence dominant.

Because we have so much data and so.

Whereas offence, there's less data.

So we have reams and reams and reams of logs about attacks that we can train upon.

So I think there's at least a case to be made that.

There could be a defence dominant.

Machine learning that it that emerges.

So so that, you know, I don't know how much to to to place on that, but I I think it's worth floating as a as a possibility and and why why? Because we've got all this data. So like antivirus is the best example where we have just tonnes and tonnes of signatures and we can reason about altered malware based on the size of our.

Database there.

### P24: Somewhat disagree

For response to accidents or attacks.

I somewhat disagree with that one. I I think it's very it's very catastrophic it it also depends on like how do you address.

Like in parallel, some of these things can be.

I don't know like address beforehand, let's say.

## Question: Attacks via Humans

**Description**: Towards 2040, cyberattacks will increasingly involve humans as well as machines, both insider threats and attackers focusing on human vulnerabilities such as taking advantage of weak passwords or manipulating people into taking inappropriate actions, even when the software works as specified.

Totals

No Opinion: 4

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 6

Strongly agree: 10

### P3: Somewhat agree

Yeah, I mean I you know the, the the sort of general sort of consensus is that.

Human factors. The human is the weakest link sort of thing and I I can't see. I can't see the sort of as long as we have humans in the loop.

I can't see that that desire or that option for adversaries to exploit that going away.

I mean easy.

Yeah, exactly.

Mean I I always kind of say this, though I think that, you know, there's a bit of a.

I mean, I don't. I, you know, I've never really seen studies of this, but I still think, you know, there's this kind of mantra in cybersecurity that the humans are the, you know, stupid users, that sort of thing. Right. And now we think, actually, they're probably, if you want diversity and resilience.

Yeah, exactly. Yeah. That thing. Yeah.

Right, yeah.

It's a sort of shortcoming of the technologists rather than. Yeah, we're doing our job bad and blaming others for being stupid.

### P4: Somewhat disagree

Yeah, yeah, it's it's the the the contention is with the word increasingly, I think they will involve them, but I don't think it's going to be.

### P5: Strongly agree

You absolutely do. And you know, when we teach cybersecurity all around the world, all the time, we always ask people.

What do you think is the most important that you should put your resources to people, technology or processes?

And it's always people #1 because that's where we think the biggest vulnerability. And on the flip side, where the most what we call bang for the buck or bang for the pound, I guess comes from is from the humans.

And so, but at the same time, you know, they're very vulnerable.

So I'm gonna say yes. Fully yes on that.

### P6: Strongly agree

### P7: Strongly agree

Yes, I talked to my humans again. This is something. This is something that's already happening. I mean, the the main attacks or breaches that happen in CNI systems happen through social engineering, so.

Is that weak passwords type of thing or install this software type of thing? Yeah.

This all of these? Yes, and and targeted phishing attacks.

### P8: Strongly agree

Just now I just say this to the psychology and this whole thing manipulating people in the city. It has a definition. It's called social engineering. They are doing it very well. They are doing it very well at the moment. Sociotechnical problems this might I have a whole paper about it.

### P9: Somewhat agree

Got it. Yes, yes. And does is that the same for the next 1-2 cascading problems?

Attacks by humans sociotechnical again, yes, these are ones that that we may well be addressing pretty well or we may not be. Yes. Yes, got it. Yeah.

That's right. Yeah. We're increasing the opportunity, but we might also be increasing the resilience at the same time and therefore managing that.

### P10: Strongly agree

### P11: Somewhat agree

### P12: Strongly agree

### P13: Strongly agree

### P14: No opinion

### P15: No opinion

### P16: Strongly agree

### P17: Somewhat agree

Obviously the human vector, the human fact. Sorry. The human factor is still quite a key one it's still quite a high one.

### P18: No opinion

### P19: Somewhat disagree

### P20: Strongly agree

### P21: Strongly agree

### P22: Somewhat agree

### P23: No opinion

But I see and I kind of think that what if you look at what's happening in?

One of the answers to the deep fake problem is to embed.

A kind of hashing into photographs into media and there's this very big collaboration to do this kind of end to end.

System of embedding.

A hash that allows editing but not falsification.

Can't remember what the group is called, but Geddy is is got money in it like all the you know, blah blah blah and I I actually imagine in a near term that we are going to have to have some type of device that authenticates us like even on like this call and it could be a device that I wear that that is in the view of the camera that basically makes it apparent if you change the video.

Based on its emission, or so on and and I think I think I think we'll start seeing politicians have something like that by 2040 for sure.

### P24: Somewhat agree

## Question: Sociotechnical problems

**Description**: By 2040, digitisation and the increased complexity of systems—including the operators and responses of users—will lead to increasing accidents despite all the participants working in good faith (as happened in the Three Mile Island and Chernobyl incidents).

Totals

No Opinion: 3

Strongly disagree: 1

Somewhat disagree: 4

Somewhat agree: 6

Strongly agree: 8

### P3: Strongly disagree

Yeah, I I think this is probably a little bit of the argument that I had before, where as I think there will, I think.

I think there's a sort of suggestion here is that.

But you know that you because cause systems are complex. Humans will sort of not be able to understand it proper, understand them properly and under into stupid decisions, right, which which lead to accidents or incorrect decision which lead to accidents. And I kind of think that's probably not going to not going to be the case. I kind of don't think that's.

I think there's a sort of systems engineering sort of perspective, you know, all these kind of stuff around great approach and stuff like this.

I think there's a risk of it if we don't, if we don't.

Design these systems well.

Right. But I I I think we know how to do it more or less.

Are you with?

I think it's maybe the word accidents I think perhaps was a sort of I think you know there might be kind of outages or failures or mistakes made.

Will they lead to an accident? Cause accident is like the, you know, the the really bad thing that you don't want to happen.

And my my my feeling is is that probably not accidents.

Disruptive service potentially or optimal operation potentially you know those sort of kind of not the sort of very extreme end of of things going sideways.

Yeah, yeah, yeah. Mine mine's auto. General Sense is that's getting better at it, but yeah.

Yeah. No, but, but yeah, so the risk, I think, yeah, social technical problems are going back to the point I made earlier. I think, you know, the threat is that way. I think, you know, maintaining is highly skilled or skilled workforce.

To handle this sort of stuff, I think it's definitely an issue, a risk.

### P4: Somewhat disagree

We've had social technical problems since the very first definition of a social technical system with with coal mining.

### P5: Somewhat agree

OK, so I think we already live in a very complex world of systems that we're already operating in.

I'm not sure I see that that's leading to increasing accidents at this point in time. Right now, I I wouldn't blame the complexity yet.

But I think for right now and now, is this supposed to be out five or ten years by 2040? OK, I'll do that. I will say that there is there is a chance that that.

Could be an issue.

I will say that much. I don't want to go full blast, but I think a little bit.

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

Technical is simply about don't only try to solve this \*\*\*\* through the technical, but also look at the socialistic and organisational factors organisation factors. Please note it down as well. Yeah, organisational factors, a job design, job design and organisation factors because the people don't work individually. Let's say what I'm trying to say, good faith. You may think of the humans good faith to the system. It could be that one human's good faith to the system but another human is trusting their colleague.

Because the human to human faith as well. So if I do one mistake here, if they trust me, especially if I haven't done anything wrong before, if you like, there is. It is a domino effect. It goes through the, especially in in industry it is a hierarchy. For example, you're talking about the chainable and and in three mile in defence it's more in military is more how many times you saw somebody's challenge in their commander it's it's just not going to happen or the frontline guys.

In terms of to working in good faith, I trust the system, whatever and human to human, and it's not even the person rank to rank. If you go to the channel bill or military particular, say, military organisation factors are different than finals. Banking is different than the issues you might have in rail. So please look into this sector by sector. Could you kind of throw the examples that 3 Miles Island and China but they are one industry.

So just what I mean in finance, there might be more independent or they might be trusting that frontline worker more who might only have 3 month training immediately, not like this, the most trusted person is the most experienced one in railway. It is not like this the most trusted one is the one that you like the most. So is the culture. So. So basically what I'm trying to to throw into here is inside the culture aspect. So who is trusting who or in some industries only humans are trusting the system. They don't trust like other human.

Net because they have to trust the should, but they train that way.

So some other industries are like that. Which one, for example like on the roads like everyone trusted on system, there is no like organisation. Anyway we can talk about all day long, but please look for it in this tool by industry it's quite important.

### P9: Somewhat agree

Got it. Yes, yes. And does is that the same for the next 1-2 cascading problems?

Attacks by humans sociotechnical again, yes, these are ones that that we may well be addressing pretty well or we may not be. Yes. Yes, got it. Yeah.

That's right. Yeah. We're increasing the opportunity, but we might also be increasing the resilience at the same time and therefore managing that.

### P10: Strongly agree

Could and I just. I'm just straight off, I want to say that there was a little bit of. I mean it was it was, you know it has authenticity and integrity, but it's also quietly political because I don't think anyone else is going to prioritise the socio technical buttons. I there you go. So there was a little bit of strategy in there but I was I genuinely think that's important but just so that'll be at the bottom of everyone else's. So I wanted to kind of be the correcting factor but that will be an outlier but that's what I was doing. I genuinely think they're important but also I was thinking politically so just just so you know I'm I'm not ignorant to to my own own kind of you know ludic qualities here.

Some other people have agreed that they're they're important. What they haven't agreed. What they didn't agree was that sociotechnical research was necessarily going to do anything about it. That was, yes, yes. You know, pointing out that we've been doing this for 20 years and, you know, yeah, it does have an impact. But, you know, the problem is still there.

### P11: Strongly agree

### P12: Strongly agree

Since your technical problems, operators will each increasing accidents or participants are working in good faith. Yeah, totally. That's true.

Almost everyone's always is working in good faith through almost all accidents like Fukushima. Everything.

### P13: Somewhat disagree

I mean, I I I think so.

So I went. There's always this thing of complexity, isn't there? And the more complex you make something, the harder it is to understand how it works.

For the greater chance of error.

But I I mean what I was thinking here that.

Would people?

So if you think about risk and assess and the risk of something going wrong in a nuclear reactor, the reactor is the impact is so high that actually that informs the design risks you would actually take. And so.

Again, I'm slightly optimistic that the people designing these things will understand that risk and design them appropriately, which would not increase complexity beyond the level which can be safely analysed.

That that sounds eminently plausible, and I've had similar comments from others actually that that, yeah. So along the same lines that the the people authorising them and creating them just don't lead, don't do complexity in user interfaces. Yes. Yeah, yeah.

Yeah, yeah. And summary, just because you can do something doesn't mean you should do something.

### P14: No opinion

Similarly, the socio technical problems is now so this is no opinions whether it's going up or down. It's it's. Yeah, exactly.

### P15: No opinion

Arguably all such incidents are sociotechnical!!! And also arguably not ALL participants acted in good faith, or they were making decisions based on different sets pf priorities.

Issue and then we go to some more attacks later on and sort of six and seven I think so it would probably be more useful if you also if you're trying to do the So what of all of this then would probably be dealt better between somebody's intentionally trying to do something nasty which tends to get dealt with by security, somebody tends somebody's done something by accident, tends to get dealt with by training and exercising and HR.

And and safety.

Oh, I mean, this is a bit of a tangent, but Gabrielle Hesht writes very interesting around the nuclear industry and the fact that.

She talks about nuclear things are either made out to be so exceptional because they're so exceptionally sort of strange and weird and wonderful that they are above all the normal rules and regulations that if you can do things you wouldn't normally do because it's so exceptional or it becomes sort of embroiled as a sort of yellow cake and a commodity that's traded, that's kind of like you can't really see where it's come from and it becomes so banal that you don't notice it and it doesn't get registered as anything.

At all, and therefore kind of goes under the radar and then somebody else has sort of picked up on that. I can't remember the name of the academic, but she was saying in the nuclear industry, this sort of.

Finalisation of this is picked up by security culture, where things like high risk things are made to be so sort of normalised within working practise. They sort of like adjust ingrained as things that you do and so certain nuclear things go into the safety area, in which case they're managed. There's a really boring normal thing and certain certain things become sort of exceptionalized and are managed under security banners.

And not even that. But I I suspect that if you looked if you were to categorise who would pick up on dealing with these these different risks in some senses a load of them would be treated as probably security risks, security threats and and therefore they are treated with a certain narrative about who it is who's trying to do that, how, how, what success looks like, what is acceptable as a as a mechanism as a mitigation and a control to manage that risk.

And the other the other side of things is, oh, it's a benign thing and you can see you're on #3 sociotechnical issues will lead to increasing instances by all the participants working in good faith. I would argue that not all participants will have worked in good faith. And I don't know who's defining the good faith.

Because sometimes and again, there's really interesting research around why mistakes happen, and sometimes because and particularly in high risk industries where there are protocols for things, sometimes it's impossible to adhere to all the protocols at one time because they're contradictory. So you have to choose a route through random other time. And so you are knowingly doing something that you know you shouldn't do, but not for a malicious reason just because it's impossible to do what you should do or all of it.

Or within the time frame, or you might knowingly do it, but you think it's the right thing to do anyway, or you might knowingly do it because you think it's the right thing to do it anyway and ever, ever, just what everybody does.

Or you might think that you're doing the right thing.

And just be doing the wrong thing, not realising it. There's various different routes for how you can end up with the wrong thing going on and and that is all like in three Mile Island and Chernobyl. A lot of that was around the interfaces.

And there were so many different things where there's no, like single root cause for these things that they're like the consequences of lots of things happening all together. So I would just argue with just the statement all the participants worked in good faith. Sorry. That was a very long winded way of saying that.

I would argue that very few people were trying to do anything malicious in those things, but then also how they were responded either to 'cause it in the 1st place or to respond to it. But sometimes the response to it also causes further things.

The all the implants.

Yes, which we did with which which did sort of come out there. So good faith is so good. Faith might be a bad phrase. But but if you said we're not trying to cause harm, I suspect is it's a sort of negative thing that people were trying to do their jobs rather than cause an upset.

Not even that there was, yes.

You I don't think you can categorically say that we're trying to do their jobs, but you could probably say like incidents that weren't directly caused by malicious intent.

And that leaves the door open that somebody could have been a bit spiteful at some point and some part of that incident may have been slightly sabotaged by something.

It was the all and the working in good faith 'cause. I don't know that you as as much as it might look like. I don't think you can say that it was true.

### P16: Strongly agree

### P17: Somewhat agree

So that's that's in, that's in Creation and OT tax are up there, but they're not as high as it should be. I'm not saying it should be, but that they're not as high in my viewpoint, they're still there, but social techno technological problems still seem to be quite an evident issue with a lot of the, you know, if you look at the social aspects of attacks which seem to be the more common forms of attacks at the moment and that that still is quite a big risk in the moment. Yeah, that was my, my viewpoint really.

### P18: Somewhat disagree

Umm. But I would digitization. Increase complexity is to include operations and will lead to increasing. Yeah. Again it's that. Yeah, there there will be uh increased risk of that. But it's important that we design systems that that make sure it's resilient to it.

Has to be, you know, if it's created gonna have to. There's no ifs or buts. It needs to be so end of. Yeah.

It's like it's like that's like saying sort of.

Let's tolerate the use of AI in in nuclear power control systems or protection systems.

And that's not particularly bothered about, you know, if the AI doesn't do what we want it to do. And I'm sorry.

That's not, that's not acceptable. Society shouldn't be accepting that sort of stuff. Yeah.

### P19: Somewhat agree

for humans like the human issue in here isn't necessarily attacks.

It's it's about people being involuntarily.

Not understanding what what they're doing or being social engineered.

Or whatever and this also to me includes.

Organizations. Yes.

I told you that.

For the I think that

The trickle of technology to learn organizations is the important.

### P20: Somewhat agree

I'm I I'm concerned about, you know, the sorts of safety stamps that are in nuclear plants.

And I've watched the documentaries and films about three Mile Island and Chernobyl. I mean, I guess I some some of me feels like well, this is, you know, this is the the paramount Raison D'Etre ~~Raisin Dutra~~ of operation of security these things to make sure accidents don't happen. So I don't think we need to overstate the risk but whether it's in increased increasing due to in interconnectivity.

I don't know. So you know it's a tough one to determine, but I so I think that's sort of a somewhat agree for me.

### P21: No opinion

I couldn't quite trace her back where the digitisation is the problem.

But so that was sort of one of those like compared to what I'm not, I wasn't quite sure whether I would really lead to more accidents or what the the current assumption of accident levels is.

I yeah, the human is just the weakest link in the chain, I think so many times.

Yeah, I think that comes from our ransomware research where we found that if you, if you're a direct ransomware victim or one who has a.

Where there's a ransomware attack in your supply chain, you actually have the same amount of problems.

Yeah. And that's that's just quite quite many of those and often.

Those in the supply chain that can cause quite a lot of harm, or quite a quite a weakness.

They're they're not designated either C and I or like critical vendors or anything like that. And they if they slip through the cracks like that, they can still cause quite significant harm and quite widespread depending on where they sit in the supply chain. So.

### P22: Strongly agree

### P23: Somewhat agree

### P24: Somewhat disagree

Social technical problems.

In good faith.

I I have a comment regarding this one and I remember I I wrote it down. It does. Does this mean that?

Like would it be over? Yes, that overestimating the capability and benefits of digital tools lead to increasing accidents because like here, the fact that.

Operator and responses of users will lead to increasing accidents where the participants are working in good faith.

I think it comes with the with with like previous.

Like personal training and.

It's like the whole process, the whole process of a new tool or a new mechanism is also getting people involved. So if the whole process, it's well done. I don't think these things should be that frequent. So I would say that I somewhat disagree.

## Question: Cascading Problems

**Description**: Towards 2040, increased interconnectivity will mean that minor problems, or failures in non-essential elements, will sometimes escalate and affect wider, vital aspects of a system. The complexity of systems will make it difficult to identify such vulnerabilities.

Totals

No Opinion: 2

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 6

Strongly agree: 12

### P3: No opinion

Yeah. I mean, will it, I guess the the, the the issue is I think that probably that sort of thing will exist, but will there be more of it, I'm not sure.

### P4: Somewhat disagree

Increase currency will mean minor problems or failures in non essential elements will sometimes escalate and affect wider no 'cause I think the whole resilience piece is gonna get its act together at some points.

Yeah, yeah.

Yeah, yeah. Also, I will point out that we don't see many of many of these at the moment.

I mean, if a terrorist terrorist really wanted to do harm.

Does doesn't have to. You don't have to use their.

Terrorists wouldn't have to use their imagination that much about the sort of things, because people may post apocalyptic films all the time. But but. But I mean, why?

Well, I mean, if you, if you look at water, for example, police presence around clean water infrastructure is significantly greater than it is.

The wastewater infrastructure, because people know people, know what the risk of contaminating the water system will be. So I think there's a lot of stuff that actually happens already to try and address this. I think that's why I think it's somewhat disagreeing.

### P5: Somewhat agree

OK, I think this happens right now.

We have issues right now where it's really hard to.

Decide where is our safety and security.

Functions that we want to protect the most compared to those that are not as important. And there's that chain reaction 'cause they're all connected together. And so yeah, a nonessential element could have an influence and escalate, I think, to some degree some vital aspects of the system. So I'm gonna say, well, yes, I slightly agree with that.

Can't remember.

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

### P9: Somewhat agree

Got it. Yes, yes. And does is that the same for the next 1-2 cascading problems?

Attacks by humans sociotechnical again, yes, these are ones that that we may well be addressing pretty well or we may not be. Yes. Yes, got it. Yeah.

That's right. Yeah. We're increasing the opportunity, but we might also be increasing the resilience at the same time and therefore managing that.

But I thought that that point around common failures that that systemic failures that underpin systems and then cascading and complexity failures, those two things are really important.

And they are hard to fix because we don't think in systems terms very often.

### P10: Strongly agree

Yeah. So I did the five, I stopped at attacks via humans, although I do actually think that that is, you know, that is an issue. But yeah, cascading problems just because like this because I'm I'm really fascinated also almost intellectually by the problems of, you know, trophic cascades and so so of course. So that's a genuine #5, it might almost be, you know be #1. But so it that that wasn't an accident, but I did, I did the, my buck did stop at five. Yeah.

### P11: Strongly agree

### P12: Strongly agree

A skating problems? Yeah, I think that's a big issue, particularly high cascading problems and unpredictable AI. So cascading problems, you know, like again, failure from failed electricity, telecommunications. I spend a lot of time thinking about that. But those things are problems. It's the cascading problems that are problems. So failures are fine. But the cascading failures are bad. So I'm even going to demote failures from electricity. It's it's really the cascading problems that I care about.

### P13: Somewhat agree

I don't think it's gonna get worse. That's gonna get no, I mean, I. It's the same response to the previous question.

You can control this in design.

If you design things carefully.

And again it it depends on.

The risk appetite of those designers and how to what extent they then isolate these systems to avoid these cascading effects and completely open systems. Yeah, well, maybe it's a it's a problem. But then as I said, I wouldn't design these systems to be completely open.

### P14: Strongly agree

But cascading problems. Yes, you see that as a relatively increasing one. Yes, great, yes.

I do simply because of the.

More things are connected through the Internet of Things.

The more likely we have system of systems failures and problems.

### P15: No opinion

Arguably all such incidents are sociotechnical!!! And also arguably not ALL participants acted in good faith, or they were making decisions based on different sets pf priorities.

Yeah, that's interesting. OK, cascading problems already exist.

### P16: Strongly agree

And then for skating problems, yes, because we understand the skating problems a bit better. So you know and working on that and some people are developing software to try to map.

Those dependencies.

### P17: Strongly agree

### P18: Somewhat disagree

Yeah, a lot of these are. Yeah. No, a lot of these, we, we we just can't tolerate. We've gotta put the engineering in place. And if the engineering isn't in place, we don't use it.

### P19: Somewhat agree

This I mean the 1 of that's 2 or 3 for scaling problems.

It's quite technical, of course, so it could be rather close to the connected to the task

for humans like the human issue in here isn't necessarily attacks.

It's it's about people being involuntarily.

Not understanding what what they're doing or being social engineered.

Or whatever and this also to me includes.

Organizations. Yes.

I told you that.

For the I think that

The trickle of technology to learn organizations is the important.

### P20: Somewhat agree

Yeah, I think I would somewhat agree with that. I think that.

System complexity will induce.

Vulnerabilities across infrastructure that we might not completely understand.

Be able to map effectively.

### P21: Strongly agree

### P22: Strongly agree

### P23: Somewhat agree

### P24: Strongly agree

## Question: Failure from failed electricity, telecommunications or internet

**Description**: By 2040, much of CNI will not be able to function without these. For example, a widespread loss of electricity supply would prevent delivery of all of transport, communications, health services, food, and other critical services.

Totals

No Opinion: 2

Strongly disagree: 0

Somewhat disagree: 5

Somewhat agree: 5

Strongly agree: 10

### P3: Strongly agree

### P4: Somewhat disagree

Much of Dean, I will not be able to function if any of these fail 'cause there's backups for these things. I mean, it's the.

I I I think I I think a widespread loss of electric supply would be disruptive. Of course it'd be disruptive, but I don't think that would it would go as far as completely destroying.

The the sort of the, the, the, the, the, the, the supply chain. Well, not in my village anyway. And electricity goes all the time so.

We see we seem to get by.

### P5: Strongly agree

I think I 100% agree with this.

Electricity and now telecommunications and Internet, they're almost just as important to everybody. I think our Internet went out in us in our home two days ago and like literally, it was only 30 minutes and everybody in my household was was just like, oh, it can't work.

So I think that's gonna have a strong dependency for sure.

That would prevent delivery of transport comms. Health. Yeah, I think that's going to have a big influence.

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

### P9: Somewhat agree

I thought the the point actually about failing from electricity telecommunications or the Internet is an important one. Again, the reason for somewhat to somewhat agree is to say we know we know about it, so it might not happen, but if we didn't do anything about it, that's a really major problem.

It's back to that if and all of these, I think are if we didn't do anything about it, this would definitely be a big risk. But surely this is to drive us to do something about it.

### P10: Strongly agree

### P11: Strongly agree

### P12: Strongly agree

### P13: Somewhat agree

### P14: Somewhat agree

### P15: No opinion

CNI can only function at best for a limited timeframe without those things. This is a current risk it is not something new.

### P16: Somewhat disagree

And and the same with failed electricity, telecommunications or Internet. Again, I think we.

We we, we this, we, we.

There are a lot of efforts being undertaken by the operators of all these infrastructures.

They are brittle, but then they operate in an environment where they know or they can discover how to shift resources quickly. We can adapt. We have a lot more probably redundancy than we acknowledge.

So and and again, I mean I I I mentioned the pandemic, but if you look at the war in, in the Ukraine, it's really a demonstration of human ingenuity and how you can adapt very quickly with very limited resources and still tackle those massive adverse events.

So I I I think we shouldn't undersell ourselves as a as a, as a society.

### P17: Somewhat disagree

You weren't convinced by failure from failed electricity, telecoms and Internet.

It was, yeah.

Yeah. So I think my understanding is quite often we sit there and we'll we'll be like, OK, we've, we've identified cyber risks. So this is going to impact you by X. And I think the problem I have to get kind of stood back on is there's been sufficient Rams put into the system IE reliability, availability, maintainability.

And they call it P Rams now, so it's performance at the front of Rams. So the idea behind it is that engineering there should be.

If it's kind of deemed safety critical.

Whilst electricity is an example, there are aspects of electricity that kind of are critical and could be critical, as in safety critical. Sorry, I imagine that there should be enough redundancy in systems. It's not to say that it can't happen.

But I suspect there will be enough, you know.

Rams aspect that considers the fact that that they possibly couldn't happen in the next 10 to 15 years, I don't think.

### P18: Somewhat disagree

### P19: Somewhat agree

Well, I think this is this is um, this is misunderstood.

I think maybe people will understand it but electricity is but you don't probably don't

understand. How easy it is in a way to disrupt.

Electricity systems.

### P20: Somewhat disagree

Yeah. I mean, I think it just again it it depends with this one, the contingencies and resilience that's built into the system, right, I mean.

I don't think necessarily we're going to have, you know.

If you lose electricity supply that you're going to have sort of cascading failures across all these six sectors. Because I think that there's the resilience is is in the way the electricity system is designed.

So I think I might, you know, I might.

I might put that in the category of a bit, a bit of over.

Hype of the threat. But you know.

### P21: Somewhat agree

Yeah, maybe I would go strongly agree at this point.

I think that again comes.

So when we talk to people that they're, they're often keen on stressing that they're working towards more independence from these things and more resilience.

But reading it again now, I think I would probably strongly agree.

### P22: Strongly agree

And

And you know, the nuclear industry is part of that, but actually it's about keeping the electricity system going. And so the CNI depends on electricity. Then you've got our Internet. And it also depends on Internet. But you can't have the Internet without electricity.

It's exactly and you can't have telecoms without electricity.

Yeah. And, you know, a lot of these hospitals and so on, yes, they'll have backup generators and so on. And I know people who run those things and so on. But but actually, I don't think.

We've got to the point where that actually is not is not enough, it's it's it. Only you know, it'll keep. It'll keep the it'll keep the heating going, but there's an awful lot the control will be, you know, it isn't enough. There aren't enough big generators floating around. Yes.

I I think that and.

We did an interview with somebody who was the senior IT person in, I think Sussex and Surrey NHS Trust as part of our work. She's she was at that time part of F tag which is the BCS thought leadership thing and she was saying actually in her trust and there may be may be different in others by doubts.

The backup generation was a laugh because it was in a.

In a shared that was subject to flooding and was mostly inaccessible and was never tested.

Well, yes, I I think it's a little bit like the you know, like the electricity for manufacturing plants used to be the province of the gynebola hat, who was the man in the boiler room, you know, at sort of they left. And I think it's probably better, you know, to assume that the electricity supply companies will manage to keep the lights on rather than generators. I mean, generators. Yes, for a, you know, short time.

It was because, you know.

If you've got sensitive medical equipment, you know being out for 5 minutes is awful.

You know for 5 minutes generators can often, you know, come in just enough to prevent the all the equipment dying. But longer than that, you have to rely on the electricity supply.

It's the grid, it's the grid. It's the grid.

So don't buy a tie yet, because it continue. It will contribute to overloading the grid.

### P23: No opinion

### P24: Strongly agree

OK, failure from failed electricity, telecommunications or Internet. I think that's actually.

Encompassed in the previous one, so I don't know exactly why it's separate because it failing and then leading to additional problems. That's an example of a cascade problem.

## Question: Unprotected repair or diagnostic technology

**Description**: Towards 2040, the increasing use of off-the-shelf software and hardware components used in CNI will introduce vulnerabilities, especially where the components are designed without security concerns in mind. Examples would be replacement sensors with additional internet features, or ‘digital twins’ insufficiently protected.

Totals

No Opinion: 3

Strongly disagree: 0

Somewhat disagree: 6

Somewhat agree: 5

Strongly agree: 8

### P3: Strongly agree

### P4: Somewhat disagree

Now people talk about diddle and people keep bringing digital twins up all the time. I mean it's it's not. It's not new technology. It's just when the babina.

It's it's it's been around for a while, I think for a number of reasons. It's a lot easier to use and people are starting to talk about well, can we certify digital twin in lieu of something else. And those conversations are starting to happen.

But I think because they were already relatively mature technologies before, people sort of discovered them, that gives me a certain amount of confidence, hence the somewhat disagree.

### P5: Somewhat agree

So I will keep going.

OK, do I wanna be an optimist or not?

I would hope that in another 15 years.

That security concerns are designed in.

We call IT security by design.

But I don't know if I have that much confidence, so I'm gonna come down 1 notch.

And say I hope so.

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

OK. Yes. So in here, Please note there is a from human point of view this where the maintenance and the third party is becoming important not to dial it operators. All right. And that's why I mentioned in digital T vs we are focusing a lot to the third parties and maintainers, not a lot to the first operator. So it is are the supporting people. So I did you put HATD 14 in one together, but it's exactly the core of.

Why we are contributing and how we are?

Part of the digital TV you're contributing the most edges, so this is really good. You see diagnostic maintenance. This is called system maintenance, infrastructure maintenance and there are different people are looking after all different technologies. We have different robots who are looking into in railway, in diagnostic and so on anyway. So we can talk all the you know and this why at some point we talking about the people whether it is because this is something which is very much is very much overlooked.

So that area that you're talking about could I think the human going to use the system, who is looking at the background, what's going on in the, you know in the background. So this is very, very important and this where the most problems are actually happening.

### P9: Somewhat disagree

Yes, I'm I here. I I just sort of tipped over in the balance. Maybe it was because it started with a negative word at the beginning of the question rather than the others, but it was the case of I I I think.

I think the new technology is used in C and I are more likely to be recognised that they're going into C and I so we'll harden them.

So we're back to that technologies that are used in systems that we don't know are going to be C and I until it's too late, I think we're going to have a real problem with.

But if we know it's going into controlling, you know, hydrogen distribution system, I'm fairly certain that we're, you know, we're we're going to be thinking about that properly.

So hence I'm gonna say no, no, we're gonna be fine because we know about that particular risk, and we're gonna manage it.

### P10: Strongly agree

### P11: Strongly agree

### P12: No opinion

### P13: Somewhat disagree

OK, I think I think it's understanding.

Potential vulnerabilities. Understanding what components to put into a network. For example, the sensor that it's capabilities.

Analysing gets risk before you in certain network. I mean you, you, you.

Kind of. See the response to this kind of thing already. If you look at, for example, the 5G infrastructure and UK.

And US governments banning Chinese technology.

The fear of they don't know what's in it. And so yeah, there are mitigation. You can you can take I I I would expect those things.

To continue.

That approach to be, you know, beefed up.

### P14: Somewhat agree

### P15: No opinion

### P16: Strongly agree

### P17: Somewhat agree

### P18: Somewhat disagree

Diagnostic technology. It's also a new new technologies and it will pose vulnerabilities as they were not designed to secure.

Examples.

Yeah. Well, so we have to make things C and I needs to be designed so it's it, can it? It doesn't have those vulnerabilities in it. Yeah.

And better, we shouldn't reduce our standards. We should maintain our standards. That's what I'm saying. So.

### P19: Somewhat disagree

### P20: Somewhat agree

Some agree. I mean, I think again we talked about this last time, there is this renewed emphasis on security by design. So I'm hopeful that what may may make an impact. But as I said to you before, I'm entirely convinced that it will. So I think it's probably.

Yeah. I mean, I think if you're that, if you're in this industry and you're putting on replacement sensors with additional Internet features or you're producing digital fit twins, you know, unless you're, you know.

Unless you're really negligent, you've got to think about security, and there's increased policy focus and standards and and and regulation on this so.

Yeah, but again, like I'm sort of a bit sceptical about how effective it will be and whether the, you know, just the corporate irresponsibility will take over. So it's probably a somewhat employee there.

### P21: Strongly agree

### P22: Somewhat agree

### P23: No opinion

### P24: Somewhat disagree

I mean, I I somewhat disagree because it's already like putting the the new technology.

In like disadvantage against like non digital tools like it's already taken for granted that they want take into account like security concerns and it and it's already like biassing.

The the projection I don't know.

New technologies used in C and I will pose vulnerabilities as they were not designed with security concerns in mind. Well, we we don't entirely know if they were not designed with those security concerns in mind. If they are, then.

## Question: Democratisation of attacker technology

**Description**: By 2040, advanced technology will be widely available to malicious parties and lay people who, intentionally or accidentally, will cause damage on systems and infrastructure. E.g. AI enhanced attacks.

Totals

No Opinion: 1

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 10

Strongly agree: 9

### P3: Somewhat agree

Yeah, I I think that sort of thing is coming.

You know, I I I think with always these sorts of things it's a little bit of you know the adversary will do the simplest and cheapest thing.

So you know, will the, you know, will they be making use of AI? Possibly if they need to.

But if you know if, if if.

You know, if what they're doing at the minute is still sort of valid in making money, you know, if we're talking about sort of financially motivated adversaries, then yeah, what was kind of it. So I just by chance, I was listening to A and I'd recommend it. The NCSC have a a podcast, would you believe?

She's with maybe worth having a listening. Listen, if you're if you're into podcasts.

And and they were. This is a bit of a tangent perhaps. But they were talking about AI.

And adversarial use of AI.

And the sort of general, I mean, I don't know whether this is just because they have to say something along those directions, but they were sort of kind of suggesting that the the sort of.

Benefits of AI would be much better for much.

Much more widely felt. The benefits would be much more widely felt by those defenders.

Rather than the attackers, so you know, there's this, you know, we have this issue about a lack of people.

You know, problems with automation and all this kind of stuff. But while the while the attackers might sort of seek to use AI, any benefits that we would gain as defenders would be would fire out strip. That was kind of what they were suggesting fire out strip any benefit the attacker would have.

### P4: Somewhat agree

Yeah, I I I I it it is I mean there are a lot of people using this stuff that quite frankly don't understand how it works.

And if people can see a way of getting advantage from it, then.

It's into I I would like to think that.

There will be something that will inhibit this, but.

No, I think it's unless I mean, I mean cherry could take off, you know, and and and it would make a lot of this stuff redundant or if not cherry something some something similar. But there'll always be places where you can't use technology, so I'm sure someone will find a way of that.

Exploiting it.

### P5: Strongly agree

### P6: Strongly agree

### P7: Strongly agree

Yeah, that's again something that's happening even now. The democratisation of attacker technology, I mean, it doesn't to become an attacker. It doesn't even require technical skills these days. You just need a credit card.

### P8: Strongly agree

~~Immigration~~ Democratisation of attack technology.

Well, obviously even they're putting the Wi-Fi on trains, don't they? They're putting Wi-Fi on the locomotive in Turkey. Good luck with that.

### P9: Somewhat agree

### P10: Strongly agree

### P11: Strongly agree

### P12: Strongly agree

I would argue, strongly agree, but I argue you know, Packer technology is pretty widely democratised.

### P13: Strongly agree

### P14: Strongly agree

### P15: No opinion

### P16: Somewhat agree

Yeah, yeah, because so it's and that's my criminologist kind of.

Hats, you know that studying hackers? So, so yes. So technically, again in theory the tools will be able available to anyone.

So it's it's so I I so that's some strongly agree but then very few people will take advantage of them.

Be a sole availability of these tools will not be enough.

To enable those people to launch very destructive attacks because there are a number of other.

Structural factors that will be needed, people need to work in teams, so they will need to have also some social.

Skills and ability so just having access to very cheap, very easy to operate piece of malware is not sufficient.

To suddenly motivate people.

To go on the attack.

Because because people are lazy, people are busy with other things. So so the tools will be readily available. Whether they will provide more opportunities for more people to launch attacks. I don't believe so.

### P17: Somewhat agree

### P18: Somewhat disagree

I'm doing quite a lot of work on AI at the moment and you can you can. You can get it a lot of advantage of an AI.

Keep things resilient. If you design it. If you design it right, so OK. The attack vectors people using AI you know will have the benefits of it as well, and so things like attack vectors will will get more subtle and more, you know, and more effective.

But again, it's up to systems designers to ensure that.

Impact of that is minimised.

Right O this is so this is yes, but it won't necessarily Causeway it.

So. So the first part of that I completely agree with the second part of it where it says will cause damage on systems and infrastructure. And I disagree with you know we we can't, we can't allow that to happen.

And we will have the tools to make sure it doesn't. Yes.

Yep. Yeah, yeah. So it's it's the way. It's the way the questions are articulated rather than me disagreeing with the so. So, yes, democratisation of technology will increase risk. I completely agree. But but will cause damage. I disagree.

### P19: Somewhat disagree

### P20: Somewhat agree

I will somewhat agree on that. I mean I again, I think.

Probably there's going to be, you know, sort of blunt AI tools that can be used to enable cyber attacks, but probably that the more advanced stuff will be in the hands of the state apparatus. I think that's probably what we've seen so far.

No, I mean, I think it's, I think it's a concern. I think there will be, but yeah, no, this idea of non state actors and doing massively damaging cyberattacks has proved to, you know, probably not be the case. And I think it'll be the same.

### P21: Somewhat agree

I think I think we overhyped that a little bit, to be honest.

I think there's loads of cheap tools and like ready made tools available right now already so.

There are so many instructions on the dark net on how you can do a ransomware attack. There's one off like tool kits that you can launch once instead of without really knowing what you're doing to launch a ransomware attack this.

From commercial hacking tools and so on already now. So yes, I don't think that will get better, but also don't think it's quite the fundamental change that people make or like might make it to be.

Yeah, I think that it's just that if you have a little bit better understanding of how much there's already out there.

Like there's so much already available to people who are looking for things.

And you really don't have to be particularly skilled at anything to cause quite a lot of harm. And as long as you're sort of willing to deploy, for example, malware of your of your, of your networks, and I'm fine with that risk.

And you can already get ransomware as a service you there's instructions for every mischievous activity online already, so I don't.

I don't necessarily think that just 'cause there's like now AI that's that's such a game changer for.

Well, that because the bar's already pretty low.

### P22: Somewhat agree

### P23: Somewhat agree

### P24: Somewhat agree

Oh, where is it? Democratisation of attacker technology.

I had a comment with this one. Oh yes.

Advanced technology will be widely available to malicious parties and lay people who intentionally or accidentally.

Will cause damage, and systems and infrastructure OK. The fact that it says accidentally, wouldn't that be include in risk #3.

In. Yeah, the social technical terms.

But attacks from hackers would be like in any case attacks. Wouldn't they, like, get? Yeah, I don't know. It's like.

I I don't see the accidental for there, but maybe yes, you're right.

Maybe I mean, just maybe unintentionally, would be a better. Yes, that was. They're not trying to cause damage, but they might do anyway, yes.

So with this one.

Will be why that to malicious parties?

Yes. Well, I somewhat agree. It's gonna be.

Yes, like more things out there mean that they are used in a good way, but also.

I don't know. Exposure and availability also makes it more vulnerable to good and bad usage. So yes.

## Question: Software and hardware supply chain problems

**Description**: 2040 will see increasing issues with the provision of software and equipment, system maintenance and related services. There will be an increasing disconnect between technology users and developers, and between procurement and technical specialists, as well as conflicts with the commercial interests of suppliers.

Totals

No Opinion: 3

Strongly disagree: 1

Somewhat disagree: 3

Somewhat agree: 7

Strongly agree: 8

### P3: No opinion

So the nuclear industry, I think probably would admit to it, even to itself, that they're not very mature.

Handling this issue, banking sector, the finance sector is much better, apparently.

So what are they trying to do? What are they? You know, what are they? So the minute they're trying to?

I'll say all of this and I don't know if it answers your question or but maybe there's something interesting that comes out.

So the so they're they're trying to do, they're kind of trying to do supply chain mapping at the moment. So understanding their critical suppliers.

And and and sort of map that out and I I kind of have in my head some sort of graph so they have like Tier 1 Tier 2 suppliers and all and all this kind of stuff.

And what are the challenges they're facing there? So one is sort of ownership of the problem.

Internally so.

Yeah. Yeah. So. So who who actually owns the problem?

Because there's and some of that is about expertise.

Right. So procurement don't necessarily have the expertise, so it's it's the asset owner that sort of needs to get involved.

Now the question is, does the asset owner have?

You know the knowledge also so, so you know there's. So there's a there's a sort of you know there's this sort of asset owner which might be an engineer or an operator or some system owner or something like that. Then there's you know they have some influence on what's been purchased. Then there's the sort of security security people.

The Security Operations Centre or whatever it is within the organisation that obviously you know don't have the domain knowledge necessarily of the asset owner, but have the cyber security knowledge and then there's the people at procurement.

But in the in the end of the ones that are responsible for executing the contract and everything else, and and they're not neither domain experts in cyber or or whatever. So it's this kind of like.

Who should be responsible? And it seems to me like the kind of getting to the stage where they're understanding that it needs to be all of these parties.

In some way.

And what they're trying to do is sort of to keep using this expression BAU or this business as usual.

So how do you how do you make all of this part of business as usual?

You know, without sort of.

'Cause the the the issue is that I think in general people are busy and we're asking them to do something new.

Potentially.

So how do we kind of minimise the overhead? Yeah.

Yeah. Yeah, it's potentially, yeah.

So yeah, and and and. Yeah. So how do we do that kind of effectively?

Yeah, it's complicated. Yeah, maybe it will get worse, but yeah. But I would, I would say, yeah, I would say generally we're kind of my sense is, is that we're still at the very beginning of this.

Yeah, exactly. Yeah. Organisations are much more. I mean, maybe that's because I don't have a perspective on it from that from that world, but.

But I you know, I I look at the supply chain issue, I don't think the issue is a technical challenge that we need to all. We all need to overcome.

It's an organisation and cultural.

And maybe there are technical solutions that support that right? But that's not the crux of the problem, I think.

### P4: Somewhat disagree

I I think if anything it will get better rather than worse. I mean already. So if if you look at aerospace systems for example, I mean the they used to be, they used to be fed. So if you look at an aircraft, it used to be about federation, now it's about integrated modular avionics. There's a lot more standardisation going in to make it a lot easier to sort of plan to sort of plug things in because the assumption is you're going to have a disparate supply chain and you have to be able to do this stuff.

And for that reason.

People are thinking about, you know, if we're gonna deploy new capability, how can we do that given it'll be a sort of heterogeneous environment?

So if there are issues with provision, it's because it's gonna be before something else. But these where there's demand for things, there's always going to be.

Difficulty getting.

So you see a trend towards interconnectivity, standardisation of interfaces, that sort of thing, yeah.

Yeah, because again, it's in the market's interest and it's in the ecosystems interest for that, for that to be exist. I mean, if you look at, if you look at electric cars sort of charging electric cars, you've got, I didn't, I didn't realise this until I was reviewing a paper recently. There are standards and protocols around that, you know, so if you if you've where they've got a Tesla or whatever, there's a decent chance you if you're driving on the motorway, you can, you'll go to electric filling point and you'll be able to sort of fill up. There's a lot of stuff that's actually happening on the software.

To make that happening, make it happening and to make it make it happen safely. But you know it's kind of appeared, you know, it's I mean when when things are going well, there's never really a fanfare. It just you just you start noticing there's there's a lot more electric cars on the road. There's a lot more charging.

Supply chain issues, I think are.

Are important simply because not not so much a risk of what goes wrong, but.

If we can get a healthy supply chain.

Then that could give us competitive advantage as a nation, given given other things that we we've got. So if you look at Russia at the moment, you know they've spun up their military industrial base to like 440%. You can argue about how sustainable.

If we have the ability to to sort it, if we had a healthy, robust.

Supply chain. That's good. So anything that would get in the way of that or would inhibit that is warrants investigation.

Anything else reading? I think that's just really jumping out at me, but that's just, that's just me, this is my perspective.

### P5: Somewhat agree

Again, this is like a a wishful thinking.

I hope we get better in supply chain right now. Supply chain is an issue. I know a lot of people are working on it to make it better, so I'm going to hope that in 15 years it's only slightly.

Gonna be still a problem.

As opposed to still like right now today I think it's right here. But I think in 15 years it I hope it gets to be just slightly a problem.

Not a big problem, OK?

### P6: Strongly agree

### P7: Strongly agree

See supply chain.

Yeah, well, yeah, that I I do agree with that as well. Supply chain is not, it's not just that of course it's because of the international.

Supply chain of the the entire sort of semiconductor spectrum, which is more and more of the door level devices being produced abroad, right?

[so you kind of have no control over this]

It's it's supply chain, it's just it's certain. I would say the sort of lower levels of the supply chain.

So more like devices and services.

But devices, semiconductors are are are mainly produced abroad. I mean, you know.

Do we produce CPU ~~using~~ the in the UK? Maybe arm but?

Even even arm, I'm not so sure. All the supply chain is is sort of UK based.

### P8: Strongly agree

The software hardware.

Users, developers and maintainers consent and definitely yeah. Israel is the commercial interests of supply. This is what they're talking about. Third party. So when I say third party, that's what I mean. It's exactly the suppliers and so on. I definitely agree with that software and hardware separate problems. So there's a whole new topic we can do.

### P9: Somewhat agree

### P10: Strongly agree

### P11: Strongly agree

### P12: Strongly agree

### P13: Somewhat disagree

And so for the same reason, you're not so worried about software and hardware supply chain problems because that, you know, we're seeing that being beefed up, yes.

Yeah, exactly, exactly the same thing, basically, yeah.

### P14: Somewhat agree

I can see this makes sense, I just don't know enough about it to be a real expert. But yeah, I I would agree with that.

### P15: No opinion

### P16: Strongly agree

### P17: Somewhat agree

### P18: Somewhat agree

Yeah. Yeah, it's I. Yeah, I agree with that statement.

You.

We're seeing that now in in AI. You know where you've got an AI developer, a software, the user, and you got the data centres and the different.

Kind of remits of those those organisations have mean it's very difficult to manage.

That complex supply chain and you know which, which means that you end up with vulnerabilities. So yeah, I'm agreeing with that statement.

The the the thing I'm agreeing with that one because it there's no. So what's in that you're saying that that will happen, you know, on on the other ones, a lot of those. Are you saying it would result in something?

### P19: Somewhat disagree

### P20: Somewhat agree

I'm gonna think again. I'm. I'm on the side of agreeing with that statement.

Do you take the complexity of the supply chains and?

### P21: No opinion

### P22: Somewhat agree

Runs. Then you see. I think once you put in your.

Cni contacts but off the shelf hardware and software is what it's about.

Your .8 under risks identified.

Sort of makes sense.

But it's not a disconnect between technology users and developers. It's about it's about procurement and technical specialists, because if you're buying stuff in it, it's about just procurement. Actually, you know what they're buying.

### P23: Strongly agree

Police in Brussels have raided a Chinese security firm this morning.

This apparently it's a firm that provides the scanners for like luggage at airports.

Yeah. So the the supply chain stuff is really scary to think that, you know, maybe my physical security is dependent upon a Chinese made.

That is sending all your information direct to somebody who has an interest.

### P24: Strongly disagree

I I don't. Yes, I have here like, why and?

But I think right now many things are already like yes, not built in house or developed.

## Question: Common mode failures

**Description**: Towards 2040, geographically dispersed systems will increasingly have monoculture technologies (systems, components and vendors) for portions of their operations, which will share the same vulnerabilities. These will allow mass replicated attacks or lead to other mass failures.

Totals

No Opinion: 2

Strongly disagree: 0

Somewhat disagree: 6

Somewhat agree: 6

Strongly agree: 8

### P3: Strongly agree

### P4: Somewhat disagree

Oh, I am configure oh common mode failures, failures happened. They are of course a concern in in, in, in, in in safety it's. But what gives me promise is the fact that we're talking about them. This isn't just something safety people are talking about. And the fact that you are starting to think about this and people are starting to to resilient people are starting to get interested in it.

People are going to think a little bit more about strategy is to sort of deal with it, whether it's.

Name or diversity of software or monitoring, or any one of a number of.

Stuff is happening.

### P5: Strongly agree

And I'm gonna say this for now because again.

It's too easy for people just to buy all the same vendor, same software, same everything and throw it out there everywhere.

For some of the safety and security systems, we talk about diversity and you don't want to have the same vendor everywhere. But again, that adds cost.

So I'm gonna say I think this.

Yeah, it is.

Yes, that's right. But I think that another 15 years, we're not gonna move much off of this today. I think this is today and I think it's also gonna remain in 15 years.

### P6: Strongly agree

### P7: Somewhat disagree

Common mode failure.

Yeah, this one I'm not so sure in the sense. So the common mode failures right in the sense that CC and I systems.

Are fairly.

Are fairly bespoke.

So it takes, takes, takes a lot of effort to do a proper attack on a CNA system and usually.

They're not sort of replicated in the sense that, you know, the social engineering and the customization of the attack itself has to do with a specific of the system that an adversary manages to understand or identify.

And I think this is this is.

What what saves us in a sense?

'Cause. Otherwise you know if you could run a warm and impact all all C and I systems that would be disastrous.

So that tends to you're thinking that tends not to be the case in large scale infrastructure. It might be the case in transport or something, but not not in what what we're talking about. Yeah, yeah.

See and I. Yeah, I don't I I wouldn't. I wouldn't think that, CNI.

Cni systems are.

Are sort of vulnerable to blanket.

I mean, not least because, you know, if you, if you, if you find the a a warm tight vulnerability in a on a Windows system.

You know you can. You can run it across the Internet and affect as many as many affectable systems as possible. It's not. It's not that simple. With without tea and and and specific.

You know specifics, instantiations of of systems.

### P8: Strongly agree

### P9: Somewhat agree

It's back to that if and all of these, I think are if we didn't do anything about it, this would definitely be a big risk. But surely this is to drive us to do something about it.

But I thought that that point around common failures that that systemic failures that underpin systems and then cascading and complexity failures, those two things are really important.

And they are hard to fix because we don't think in systems terms very often.

### P10: Strongly agree

### P11: Strongly agree

### P12: Strongly agree

### P13: Strongly agree

### P14: Somewhat agree

### P15: No opinion

### P16: Somewhat disagree

Common mode failure. Same reasons that I mentioned previously.

Adaptive capacities I think can and when we've seen instances with with those big.

Zero Day exploits or you know, Internet vulnerability that were discovered and that seem to threaten the whole Internet or the whole.

Operations and we're able to fix to patch very quickly and people did, you know overnight shifts and and weekends were ruined. But in the end we we kept the Internet operating. So I'm not saying it it cannot happen.

But I don't think there is any certainty in that and the the the odds are very slim I I mean.

If yeah, so it's yeah. So just to clarify, when I'm saying, somewhat disagree, I'm not saying it cannot happen. It will happen. That's a statistical certainty, but we should factor in our ability, our response and recovery capacities into the and that's what my somewhat disagree response tries to capture.

### P17: Somewhat disagree

you're not convinced by common mode mode failures?

Yes, exactly. Yeah, so I think.

But what I understand the OT cyber security market as well as the OT market in general.

Is going to get quite proportionally bigger and it's it's relatively small to its counterpart, which is the IT market in that sense. So I think the range of technologies will be more.

More, more kind of diverse, so I don't think there'll be a sort of dependency on common components if that makes sense. So the right necessarily have the same sets of vulnerabilities that are shared across all systems.

That's why I was sort of kind of disagreeing with that on that sense.

### P18: Somewhat agree

Yeah. So I strongly agree with that. I mean it I will, yeah. No, I've, I've, I've agreed with that. I've agreed with that and not you're the one so to geography dispersed systems will increase and rely on the same technologies. I agree with that proportions of their operations. Agreed, which will share the same vulnerabilities. I completely agree with that. These will allow mass replicated attacks. Yes. Agree with that.

Or lead to mass failures and agree with that. Yeah. So I do agree with that.

Yeah, that's sort of saying about the software, you know, very difficult to make it resilient. So the only way of doing it is to have two separate types of software doing doing something.

So if you have everything with the same system, then everything becomes vulnerable to the same to the same failure.

### P19: Somewhat disagree

### P20: Somewhat agree

Yeah. Again, you know, you're not gonna have completely bespoke systems operating across all these different areas, so.

Again, it sort of depends on what you mean by geographically dispersed. You're talking about the same company having operations in multiple countries. Or are you talking about different entities or organisations using the same technology?

I think I I think that that's probably still gonna be the case, so yeah.

### P21: No opinion

### P22: Somewhat agree

I know that looking at #9, the National Preparedness Commission is worried about that.

And that's an important one.

### P23: Somewhat agree

### P24: Somewhat disagree

I would say again this is a cascade failure being originated by the fact that it's it's like 1 common supplier.

Like the but the. But here we saying the risk. So I would say this would be a cause of the same risk like a different cause of the risk.

Oh no, this was the previous one. Geographically dispersed systems will, but isn't that happening already like that? Systems have just one supplier so.

Projecting things that are already happening right now.

## Question: Magnification of problems through social media

**Description**: By 2040, issues of misinformation and disinformation will escalate relatively small problems into mass panics, which then cause further failures (this was a feature of the Colonial pipeline incident).

Totals

No Opinion: 3

Strongly disagree: 0

Somewhat disagree: 4

Somewhat agree: 9

Strongly agree: 6

### P3: No opinion

### P4: Somewhat disagree

That's that's you. People are running out of petrol is a pandemic. Let's go and buy more toilet paper.

I mean, there are state nations that use MIT that use misinformation as, as, as a matter of course. And I think the EI think the environment will will evolve strategies for actually sort of dealing with it.

That, that, that's just my view because that there I think because I think there are enough people interested in the problem.

That stuff will will. That stuff will help address it.

Yeah, yeah.

### P5: Strongly agree

You know, I think it's only gonna get worse.

We have a lot of discussions right now about misinformation, disinformation.

Yeah. Oh, absolutely, absolutely.

Man, so like deep fakes. You know, deep fakes are.

So you know and and with elections there is so much fear right now in our election coming up of misinformation and disinformation that you can see a video of somebody that you think is one of your politicians that you like or don't like saying anything in the right voice, the right look. And that could persuade you down.

My my bottom line is people aren't gonna know what is the truth anymore and I think that will have a huge impact and could cause mass panic.

So I don't see that changing in the next 15 years, to be honest.

I think we have a ways to go on that yet.

### P6: Strongly agree

### P7: Strongly agree

That that is a magnification. Yes, it's it's already is. I mean, some sectors say that even if we're not, even if we we we're not under attack. If someone claims we are the reputational damage is enough.

To not to shut down the sector. But it's.

That's right. Yes, that's a whole new form of attack, isn't it? Yes, yes.

### P8: Strongly agree

I will say, yeah, why not strongly the magnification?

Now the panic attack. We studied dead in the context of generally trapped a train in the middle of a tunnel, so the mass panic where people are jumping out of the train, you can Take Me Out of the train, out of the building. You can put me in a country. You can put me. It can expand because the human panicking is very corded so definitely misinformation, malicious information, misleading panic. And by the way, let's talk about this later on. This also depending on type of humans.

Identified who is going to be panicking first, we're going to do the first error. So what kind of humans? What? Which ones are more vulnerable? Do you know that often? Do you know the more experienced you are, the older people or you are disabled? You are less susceptible, but the ones who are confident, confidence, youth, you know, these are the things they can.

Deactivize if they can't react faster anyway, we can talk about. Yeah. Yeah. Terminated somewhere.

I don't know. You know, I somehow agree. I don't know. It might be.

### P9: Strongly agree

Yes. So something I do, I do genuinely agree is going to be an issue and it's going to be very little for us to. It's going to be very difficult for us to do anything about. It is in the information domain rather than the data and technical domain if you like.

The things like the colonial pipeline incident, they matter, things like the Hoo ha around, the destruction of the gas pipelines in the Baltic Sea.

Things like the dredging up of cables in the Red Sea.

The public discourse about those.

Is enormously damaging. Governments in the West aren't trusted by their populations to be on top of these problems.

One might say likely so, and it's part of being in a democracy, but it means that part of managing the problem has got to be managing the debate and the conversation, and that's really, really hard.

So it's under the risk of particularly with these sorts of issues, the risk of panic and toilet rolls during COVID.

Right, you know.

So I think I think we'll, we'll we'll spend more time managing those things than I think we we would like.

So that's avoided by not having anything break in the first part. That's fine.

Right. But it becomes a very important part of resilience. Presumably, yes, yes, yes.

### P10: Strongly agree

### P11: Somewhat agree

### P12: Somewhat agree

magnification problems with social media. God I I guess I agree with this but I also feel like there's always a world where.

There's a backlash against social media and social media is much like we're some peak social media usage, just like we were at peak smoking, you know.

Thing, but really you think it's it's like it's.

I'm not. I don't think it's binding. It's probable, but it's definitely possible.

### P13: Somewhat disagree

No, actually, I I I think by think I think.

There was a shift underway and the population that.

People understand that social media is full of disinformation and increasingly aware.

I mean, I think that initial phase of.

Oh, isn't this sharing thing right? Let's put everything out there as long as it's dissipated and given way to a lot more scepticism in the population.

A lot more.

Not taking things at face value, so I thought I think that shift is under way.

And by 24, I think social media will look very, very different actually.

### P14: Somewhat disagree

Why do I somewhat disagree? Because.

This information is such a big issue now.

I do. First of all, I wonder if we're gonna be getting better at.

Country it.

Secondly, I question the idea that it causes mass panics again because people in a more resilient society.

You know it's you get the sort of blitz mentality where people don't panic.

And part of this could be cultural. Some societies or cultures are more likely to panic than others. We in Britain tend not to be a panicking culture.

So I didn't feel persuaded by that.

### P15: No opinion

### P16: Somewhat agree

Yes, so somewhat agree. So I think it's it's it's a, it's a it's a major issue actually maybe I've so I've been reading more about this information lately and maybe I would revisit that one and and and and and probably more agree but.

Mass panics is maybe the the term that.

Made me go with the somewhat disagree because I think people the problem is not mass panics. It's like indifference.

Or people not paying attention anymore.

About massive problems.

And being.

Prisoners into this entertainment bubbles and paying less and less attention to political or environmental or security problems.

So I don't. I don't see. I see people.

Isolating themselves away from those big mass panics and saying, you know it's as as as long as they are able to keep on living their comfortable lives. And I'm speaking more of Western countries, I don't see now anyone being panicked about much.

Because they can kind of. You see what I mean? You know they can.

Live their life in, in their kind of.

Bubble philtres where they can keep out what makes them uncomfortable, and they can just see what is of interest to them or relieve them from anxiety. So. So I don't see any moral panic happening anymore, which is probably not good because if if it was the case, maybe we would have more action on the environment and and you know, so. So I think it's.

We have the opposite of that. We are stuck into a collective action problem. We don't have enough of moral panics anymore to get people to change their behaviour.

But that's.

Yes, yes. So that's that's a very cynical. I'm I'm a political scientist by training, so it's a very cynical view of the world.

### P17: Somewhat agree

### P18: Somewhat agree

Uh, yeah, issues escalate. But let's see before.

Yeah, OK. Yeah. Well, the fact that there's an example of it, then it has to be a yes, doesn't it really? So.

### P19: Somewhat agree

### P20: Somewhat disagree

Social media issues of massage will escalate relatively small point of mass panics.

Just close your potion of mass panic.

It depends how you define, so I'm being a social scientist depends. I defined mass panic, doesn't it? You know, there weren't people running through the streets going crazy, but.

Oh, I saw. Yeah, no, I think I'm gonna have to somewhat.

Disagree with that one.

I think that language is probably wrong.

Probably not.

Doesn't capture. I mean that that would be that that suggests some mass hysteria, right? You know, obviously, you know, the probably the better example is is not mass panic, but it's the January 6th stuff at the Capitol. It's the use of disinformation to to create violent divisions, which I've written about.

But I don't think necessarily. Mass panic is the result and has been ever.

The social effect, so that's.

So I think probably mass panic is is overstated.

Social media is probably further up there and related to sociotechnical issues.

### P21: Somewhat agree

I think that's sort of similarly.

Similarly, one where it wasn't just quite sure what to compare it to.

As as some problems already.

Magnified through social media, yes, but how does that specifically CNI relate?

I do think that there's like social media, definitely by, like amplifying panics and so on. But again, I already think that's happening right now. I'm not sure whether that will grow that much stronger within 10 years.

So probably a little bit, but because more, I mean there's still growing numbers of social media users and I think less and less.

Perhaps the resilience to questions of these things, but I didn't strongly agree in the sense that I don't think of.

The starting point I think is already quite bad. I'm not sure whether we'll get that much worse in 10 years.

### P22: Somewhat agree

### P23: No opinion

### P24: Somewhat agree

Edit a little bit. The name maybe of like public misinformation.

It was maybe.

It could lead to magnification of like a simple problem or minimization of a big issue. So I would say like it's in general public misinformation.

And one of the causes would be a higher use of social media, which I agree.

## Question: Electromagnetic storm

**Description**: There is a reasonable chance, by 2040, that an electromagnetic pulse, from the sun or a distant nuclear bomb, will destroy many vital components of modern infrastructure. This may involve disabling power grids, communication systems and computer networks with catastrophic economic and social consequences.

Totals

No Opinion: 8

Strongly disagree: 0

Somewhat disagree: 5

Somewhat agree: 7

Strongly agree: 2

### P3: No opinion

### P4: Somewhat disagree

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.

### P5: No opinion

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.

### P6: Somewhat agree

### P7: Somewhat disagree

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.

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.

### P8: Somewhat agree

### P9: Somewhat agree

### P10: Strongly agree

### P11: Strongly agree

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 ½ 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.

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.

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.

Yeah, yeah. But whether it’s major or just business as usual, who knows? Yes, yeah.

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.

### P12: No opinion

### P13: Somewhat agree

### P14: Somewhat agree

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.

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.

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.

### P15: No opinion

### P16: No opinion

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.

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.

### P17: Somewhat disagree

And you’re not convinced? Moving on down to an electromatic magnetic storm.

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.

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.

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.

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.

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.

### P18: No opinion

### P19: Somewhat disagree

### P20: Somewhat disagree

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.

### P21: No opinion

### P22: Somewhat agree

### P23: No opinion

### P24: Somewhat agree

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.

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.

## Question: Radio hacks

**Description**: By 2040, connections that are currently wired—especially in nuclear—will be replaced with radio connections, leading to successful cyberattacks using radio interception.

Totals

No Opinion: 4

Strongly disagree: 3

Somewhat disagree: 6

Somewhat agree: 9

Strongly agree: 0

### P3: No opinion

### P4: Somewhat disagree

I think as they're ready protocols in place for actually dealing with them.

So I mean, I know on inland systems there are a number of well known low power protocols and you know how people might sort of try and get at those and even if they get at them, given the sort of life of the operations that they're going to support it, it's hard to see.

Impact will have not. The people won't sort of try, but.

### P5: Somewhat agree

And again, I know we're talking about all critical infrastructure right now and there is a move.

Yeah. So in nuclear, we're much slower to adopt wireless and radio for control systems and monitoring systems. However, I know the other sectors want to move more quickly.

To the wireless.

So I think yes, definitely it's gonna happen. I just don't know how quickly.

And yes, it could lead to some cyber attacks using radio. The one thing is in cyber we don't see and again I've been doing this for 20 years, we haven't seen a lot of cyberattack using radio interception very much or people aren't reporting it. We don't know which.

But it's not nearly as in the in the news as like ransomware or something like that, which typically doesn't use radio or anything like that.

So I'm just gonna I slightly agree to that.

Yeah, you're right. It's a more of a local type thing as well.

I don't know. I mean, as of today, you know, I haven't seen anything I could even disagree with some of this, but but it could. I mean, in another 15 years, I'm I here's why I say slightly agree is because there is more and more discussions all the time. I've seen a slight trend of talking about more and more wireless in critical infrastructure. So that's why I'm going to say slightly.

### P6: Somewhat agree

### P7: Somewhat disagree

Wireless again, I'm not so sure about nuclear. Are you using mentioned nuclear right?

Yeah. I'm. I'm not so sure.

But in 15 years?

Wireless would have replaced wires.

### P8: Somewhat agree

### P9: Somewhat agree

### P10: Strongly disagree

No, and this might be because I don't know enough, but I I myself you know, there's a lot of good work going on in amongst our friends.

Around around kind of radio stuff. And so I, yeah, I I'm. I'm not that worried about radio hacks that might be another complete naivete and you might have you know other people who who who know better really are but that didn't seem to me to be a you know among the kind of key risks in in in this space yeah.

Right. OK. OK.

### P11: Somewhat agree

### P12: Strongly disagree

Radio connections. Wow. Yeah. No, I I think I strongly disagree with this because I think like if they're using radio, there will be strong encryption just like they're strong encryptions, Wi-Fi. Jesus radio. Yeah, it's it's almost like, check your understanding kind of question.

### P13: Somewhat disagree

Oh, right. Yeah, I can listen in the casket of. Well, why would you do that?

Right. Oh, apparently they have reasons, but but other people are experts in nuclear also told me. Yeah, but I'm not very worried about it. You know, it's only short range radio in a power station. What do I care? Yeah, so yes. Yeah.

Again, it's it's a risk. Different thing, isn't it? It's OK. So you there's no risk or the impact is very low or the unlikely it's very unlikely event to happen then but otherwise don't use it.

### P14: Somewhat agree

### P15: No opinion

### P16: Somewhat agree

No, I don't. I don't see that.

I don't think that radio hacks.

Are I don't even know if younger people know how to operate a radio properly or.

So, so, so not not in Western countries, I don't see that happening. Maybe the the, the, the satellite or space.

Initiated hacks. I think we're seeing that.

Happening also with disruptions to the GPS signals in the Middle East that's causing really massive problems to commercial aviation. I don't, I don't know if you have that as a as a as a risk, but I would, I would say that satellite hats probably much more.

Of a concern than radio hacks.

But for me?

### P17: Somewhat disagree

you felt the same about radio hacks or radio connections being hacked

Yeah, I think radio's radio. Everyone knows radios is a bit susceptible, but I think yeah, I can't. I can't see, you know, the existing communications like some of it will be radio based and some of it will be sort of like digital switch packet based systems. So as well as like fibre as well fibre and copper kind of system. So they'll they'll you know it'll be a range of all of them really it won't just be reliant back onto kind of more old school RF.

The Rs space for communications in the event of that makes sense.

### P18: Strongly disagree

I think, well, I do. I do it. I think it off, it does have bigger big problems with this.

This we need a good replace leading to success. It's the bit at the end leading to successful cyber attacks using radio interception. So I I I agree the use of wireless is.

Increases vulnerability, but systems should be designed so that that vulnerability doesn't lead to the successful cyber attack using radio interception.

### P19: Somewhat disagree

### P20: No opinion

I don't really know about radio hacks assistant. Are they putting radio technology and nuclear power plants? I don't know.

Seems surprising to me if that's what is this like more advanced radio technology? Or is it? I mean, I don't know. I just don't know. I've not heard of that before.

### P21: No opinion

### P22: Somewhat disagree

### P23: Somewhat agree

No, it's I. So I wanna choose ones that are like not so obvious and one is radio hacks. I think that the electronic, the electronic warfare aspect of of security is.

I mean so like all these people stealing cars and stuff, that's not computer hacking. That's radio. That's like. And so I I think there's gonna be I think that's not being paid attention to.

### P24: Somewhat agree

## Question: OT attacks

**Description**: By 2040, many aspects of Operational Technology (OT) will be integrated with Information Technology (IT) and IoT (Internet of Things, or sensor technology) which will be used by cyber attackers to destroy or disable electromechanical systems.

Totals

No Opinion: 3

Strongly disagree: 1

Somewhat disagree: 1

Somewhat agree: 9

Strongly agree: 8

### P3: Strongly agree

### P4: Somewhat disagree

Well, you know we we talked about this. I mean, I remember talking about this back in 2000 and 2010.

I'm certainly at the time. Then their feeling was that number one, why would people care? And I think that's that. That's changed now. And then the second thing is the sort of level of knowledge you would need around.

Not just the technology, but how it's employed will be such that it would be non trivial. Now I think the technology associated with IoT stuff will probably will will probably find use.

Creek Creek its way in, but the actual software stack stuff might take a little bit longer and and as such I think ~~a tax~~ attacks would need to be.

Somewhat somewhat stronger.

Maybe that should be somewhat agree. I I think the attacks are gonna be there.

But it's the, but you're not. You're not saying increasing here, are you? Just that.

### P5: Strongly agree

100% It's happening now. It's gonna continue to happen.

Yeah, there's gonna be a blur pretty soon. Of all of this.

### P6: Strongly agree

### P7: Strongly agree

Yeah, I think that's yeah, the OT attacks I think is an issue.

### P8: Somewhat agree

### P9: Somewhat agree

### P10: Strongly agree

### P11: Strongly agree

### P12: Strongly agree

Ito Yeah, we already live in that world.

### P13: Somewhat agree

Again, it's a question of how you design these things.

And being aware of the types of attacks.

So yeah, somewhat agree. I mean it's possible, but again, I think there's there's mitigation.

### P14: No opinion

### P15: No opinion

### P16: Somewhat agree

So OT attacks I think.

Somewhat agree would be in the sense that sophisticated attackers like.

Nation states will keep they've they've been using that already. They will keep on using that.

More.

Amateur.

Hackers. It's probably a bit too complicated for them.

Unless they're enabled by AI tools. But you know why go into this more complicated route when you can just launch a more direct attack into the systems of the companies. And so that's why I'm kind of not not not convinced, I mean it. But but but but but the the point he had of the problem will will remain very very pointy.

### P17: Somewhat agree

### P18: Strongly disagree

Many aspects of operation technology will be integrated with information technology and Internet of Things which will be used by cyberattacks to destroy again.

To destroy or disable, we need to design them, so that's not the case. So having data diodes in those sort of things so that they can't.

They can't. There's no way through a data diode. It's like physically possible, impossible to do it. So your OT needs to be protected from the IT using technology like that to make sure that you know the baddies can't get in there.

### P19: Somewhat agree

### P20: Strongly agree

It says strongly agree that.

Again, I you know, again I think destroy is probably a strong word, but certainly interrupts disable, disrupt, yeah.

### P21: Somewhat agree

So I think.

Generally, I think that's true and it will, but I'm also quite aware that it's actually often quite challenging to launch a cyber attack against operational technology.

That's sort of why I didn't feel like I strongly agreed because I didn't want to make it seem like.

It'll suddenly be super easy for attackers.

### P22: Somewhat agree

### P23: No opinion

### P24: Somewhat agree

## Question: Commercial dangers

**Description**: By 2040, increasingly, supplier commercial considerations will exacerbate the damage done by cyberattacks: for example unwillingness to repair, to stock components, or to supply services when the charging system is down (Colonial pipeline).

Totals

No Opinion: 5

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 6

Strongly agree: 9

### P3: No opinion

### P4: Somewhat agree

### P5: Somewhat agree

I’m gonna say slightly agree.

We did learn a lot from Colonial pipeline incident.

I would hope to think that we continue to get smarter and smarter on cyberattacks.

So I’m gonna say slightly increase.

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

### P9: Somewhat agree

I did wonder. I did pause for thought on the commercial dangers 1.

The.

So mind saying on the colonial pipeline incident, one of the challenges they had was that as soon as they understood there might be a problem. They shut the pipeline down.

In order to avoid making anything worse, and that actually made things worse, now the extent to which that was driven by corporate risk is a case of, yeah, actually we’re not very good at managing commercial risks. As organisations we you know, we like to think we are, but we’re not witnessed the 2008 financial crash.

But.

But they do try. OK, so it’s there.

If I go back to my rant about financialization and shareholder value, driving bad investment and decision making, I don’t know if that would fall under this bucket. If it does, I I want to know what the next button after strongly agree is.

But I I kind of hold it in my head in a slightly different space. This is sort of once you’ve had an incident, does your, does your knee jerk reaction get driven by your commercial interest? It’s like, well, yes, of course it does.

But but So what? I mean that’s like, you know, physics on the other hand, if you turn around and go, the whole reason this happened in the 1st place is because you’ve been rent extracting from the asset.

And you’ve deliberately placed it in a position where it’s at enormous risk, and you’re counting on the government picking up the pieces as you go. And I go, that’s that stinks. But that’s a pattern that we’re beginning to suspect it is playing out in, in various different places.

You know the utility asset owners at the moment are facing some very real choices.

Around that commercial intent because.

Let’s let’s say you’re let’s say you’ve got a massive underground asset like a gas distribution network or a water distribution network, or you’ve got sewage distribution that’s worth a lot of money at the moment because people use it. If it doesn’t have a role to play in the future energy ecosystem of the country, your asset has just disappeared.

What are your shareholders?

Why would it not be required? Sorry.

Well, if if I’ve got a gas distribution pipeline designed for methane and it turns out it’s no use for hydrogen.

When we turn off the gas supply because we suddenly turn around and say, you know, well if I’m, if I’m doing fuel distribution, if I’m driving, this is one that came up with the day. If I’m distributing petrol up and down the country and the government turns around and says actually it’s not a case of being illegal to buy an electric vehicle by to buy anything other than electric electric vehicle by 2030. But by 2040 it’ll be legal to drive anything other than electric vehicle. All of those companies have just revalued massively. Most there’s what are the shareholders going to do?

OK. So so that’s where that regulatory consistency and stuff really matters and where that messaging really matters. But those commercial pressures and commercial dangers are really, really distinct. They felt to me to be more systemic than this example, but I think they are a really big deal.

Interesting. So that’s a different sort of commercial danger rather than the yes side. Yes, that sort of commercial danger that we were talking about with kind of the.

124 hour response you were talking about a very bigger, much bigger story. Yes, yes, yeah.

The the the systemic risk, yeah, yeah.

### P10: Strongly agree

### P11: Somewhat agree

### P12: Strongly agree

### P13: Strongly agree

### P14: No opinion

### P15: No opinion

### P16: Strongly agree

### P17: Somewhat agree

### P18: No opinion

### P19: Somewhat disagree

### P20: Strongly agree

Yeah. I just think that the whole industries has a major problem with incentive like commercial incentives and profit making over security. So I think that’s going to continue to be the case. Unfortunately, I think it’s going to get any better.

Yeah, I I guess I’m prioritising more around.

By commercial dangers.

Umm.

I mean, I think that’s fundamental like it.

If it’s.

Commercial operators not doing security well or seriously. Then I’d put it right up the top, but is that what you mean?

Well, it was also the the misincentive of of when you actually have a problem, you know your commercial interests and the human interests might be quite different, yes.

### P21: Somewhat agree

Yeah, I do think.

That in the maybe maybe I only ever somewhat agree because my current assessment of things is so pessimistic.

Because I already think commercial considerations to some extent outweigh resilience and so on. Otherwise what we currently have would be stronger and better.

Most of it isn’t because the market doesn’t seem doesn’t demand more security. So I think it will. I agree with the trend or I agree with his assessment, but I don’t necessarily think that 2014 that sends as a game changer what we currently have is anything. I hope that some of the movements in the US on more binding regulation.

Developers more accountable that marks quite a big shift in the US approach and the US being the dominant player of software and so on.

Yeah, if anything, hopefully, hopefully not.

It’s an executive order by the by President Biden, and it it marks quite a shift, and similarly in the new cybersecurity strategy in the US, there’s a greater.

Acceptance that vendors and software developers hold responsibility, not just the end consumer, which is quite a drastic shift because so far it’s always been responsibility lies with the consumer.

Whereas this new shift puts more binding, more binding.

Obligations on software developers and and vendors as it ever has before, so that would be things like security by design and so on so forth. And I think with the US changing that’s quite a strong signal to the market.

Is this? Is this the one that I I heard of as the Bill of Materials, one that was a part of it? Wasn’t software bill of Materials is is it that executive order or is there another one?

A bill of materials does not ring a bell for me.

It is also in the in the national security strategy.

So that would be so’s.

So this was this was Biden.

Yeah, I would say.

Maybe a year ago.

### P22: Somewhat disagree

And to #6 and number seventh, because commercial ranges supply commercial considerations will exacerbate the damage done by cyber attacks and willingness to stock compared to supply services, I mean absolutely big danger following on from the point about.

Software and hardware supply chain problem. So that’s.

### P23: No opinion

Yeah, I I I guess I I I couldn’t. I didn’t quite understand the point. So is it the, is it the idea that colonial really shut down their pipeline because they couldn’t bill?

Yeah, I’d so I. So I mean that is a problem that the underlying, yes, I I would say I definitely agree with that Ben. I I just wasn’t sure what it meant.

I mean, there’s a deep incentive problem.

### P24: Strongly agree

## Question: Unpredictable AI

**Description**: Towards 2040, as AI is increasingly introduced, the occasional inconsistency and unreliability of AI outputs will lead to damaging accidents—whether directly in control systems, or by causing incorrect operator actions.

Totals

No Opinion: 4

Strongly disagree: 1

Somewhat disagree: 3

Somewhat agree: 6

Strongly agree: 8

### P3: Strongly disagree

Yeah, yeah, I'm kind of a bit. Yeah, sceptical that.

I yeah. I kind of got a sense that we won't find AA. What I'll do. So last week just so happens.

Maybe that's sort of a little bit influence.

By 2040, I mean my hope is that we're on top of this by 2040, but so the O&R, the regulator, the UK Nuclear Regulator, published their kind of position on AI.

And I just kind of think the way that we do regulation in the UKI, don't I just don't see AI.

You know, eventually we ultimately we end up having to make a safety case.

To find AI in control systems.

Yeah, I'm not sure. I'm not sure.

Maybe I'm just being a bit, but I what I can do, I'll send you the. It's a very short thing. I'll send you the the the kind of position.

The position on it, it's it's sort of, it's not a very long document. It's like 15 pages.

Got a very being quite proactive about it. I think like I mean I'm, I'm sounding like a bit of a sort of advocate for the regulator, but I think they've been quite smart.

So the way we do regulation in the UK is all performance based.

Right. So outcomes based.

Yeah, yeah. The performance based outcome space. So we basically have to.

So the the regulator look, you know you have to sort of make a safety case and demonstrate that your systems are safe or whatever. So there's the outcome that you have to kind of argue the case for.

And so that gives the UK regulator quite a lot of flexibility.

Terms of how they regulate things like AI in a sense sort of puts puts some onus on the on on the in in on the operator or the duty holder and the vendors and stuff like this to prove to demonstrate that.

You know, they think they can operate these things safely.

But you know, the AAI for AI point of view, you know, and are having. They're doing these things called sandpits.

Where they sort of trialling AI technologies for using nuclear, you know they're engaging with kind of researchers as well to sort of, you know, looking at AI in the use of robotics, for example, I've got to try to produce guidelines about how to, you know, develop safety cases for the use of AI mean. I don't have a strong sense about how good that is.

But you know, it's 2024 we're talking about 2040.

It feels like we're sort of switched on to it.

And we're in this sort of, yeah. So I kind of think that.

Hopefully we, you know, we won't be making stupid decisions about this, at least for nuclear, maybe in other sectors, perhaps, but.

### P4: Somewhat disagree

### P5: No opinion

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

### P9: Somewhat agree

### P10: Strongly agree

### P11: Strongly agree

### P12: Strongly agree

I'm gonna just put unpredictable AI, because that's just falls into the poisoning. Like poisoning isn't a problem. If we can predict that it has been poisoned, it is the unpredictable problem, not the poisoning. You see what I'm saying?

So, like bugs aren't a problem. Bugs aren't an issue. Bugs in production are an issue.

### P13: Strongly agree

### P14: Somewhat agree

### P15: No opinion

### P16: Somewhat disagree

No, no, I don't. I I hear all the hype AI as an enabler for attackers, but I don't. I did. I didn't understand that question as that.

Configuration and more like AI becoming.

Autonomous enough to start operating on its own, so us losing control of AI.

And.

I I don't think it's going to happen.

Oh, no, no, I don't think. I don't think that's what the unpredictable AI was about. It's more about the whole thing of not being able to test every possible situation. And so they're being glitches that would happen, yes.

Oh, OK. Well, yeah, OK, what does? OK. So then probably, I don't know. No, I don't. I I think AI is it's gonna be introduced very care. I mean it's it's.

Generative AI is gonna be introduced massively for certain tasks, but could it be used with a lot more caution for other tasks?

It's become. It's gonna become more and more reliable, I think. And we can see it already. You know, the hallucinations and all that is, is, is, is.

Instances are decreasing in terms of.

So. So yes, unpredictable. But again, there is a huge amount of people working on AI security. And so it's going to go the way of the Internet. You know, we've developed this wonderful technology with no concern for security and then a whole industry is gonna is gonna appear and then it's gonna.

Develop all kinds of control so it's not gonna be perfect, and we're gonna have incidents, but I think it can easily be contained.

### P17: Somewhat agree

### P18: Somewhat disagree

We need to be resilient to it. I mean, it will happen. Yeah, but.

So I agree with the first stage first statement, but I don't agree with the second statement. We need to prevent it.

Yeah, it is, because I think increasingly it certainly means being used now.

As a predictive.

Tool for for maintenance and stuff like that and to look at vulnerabilities and if it's ill informing then you know it's going to it's going to mean people potentially are comfortable with the way things are happening. But the true nature of it is being hidden from them. So yeah.

Yeah, we're seeing it increasingly AI being used. Yeah, yeah.

### P19: Somewhat agree

### P20: Somewhat agree

Again, it's this is 1 again that somewhat agree it's it's just depends on the capacity of how well we deal with the problem.

### P21: No opinion

### P22: Strongly agree

And then I like the fact that even though you've got an AI wonk on your groups of your team, you actually recognise that AI is likely to go, hey, what are times or just be wrong. And so I think unpredictable AI.

Occasional inconsistency and unreliability. I don't know. Did you see the Royal Institutional lectures on AI?

It was a it's a series of three held over Christmas, and it was three lectures and you know, that's they they did lots of sort of demonstrations and experiments with the ~~audit~~ audience. So it was absolutely clear, certainly at present.

And I mean, I've done tests myself on chat GBC and see what.

And you know.

So I think there is a point about unpredictable AI that because nobody can check the result occasionally, it's just going to be wrong and people will assume it's right.

### P23: No opinion

### P24: Somewhat agree

## Question: Poisoning of AI

**Description**: Towards 2040, cyberattackers will tamper with the datasets used to train AI models, causing incidents directly, or allowing ‘loopholes’ to allow the attackers access to vulnerable systems.

Totals

No Opinion: 2

Strongly disagree: 0

Somewhat disagree: 1

Somewhat agree: 12

Strongly agree: 7

### P3: Somewhat agree

### P4: Somewhat disagree

### P5: No opinion

### P6: Strongly agree

### P7: Strongly agree

### P8: Somewhat agree

### P9: Somewhat agree

### P10: Strongly agree

### P11: Strongly agree

### P12: Strongly agree

### P13: Strongly agree

Well, I, yeah, well, my yeah, but it’s it’s difficult. So it’s really difficult to write some of these things and a lot of it depends as well on how embedded I becomes. And I previously answered well, maybe not going to be so bad, but then it could be. And the thing with something like poisoning with AI, I mean it could be potentially undetectable.

And an autonomous system where you can’t detect it’s been poisoned. Then it starts making unusual decisions.

So my scepticism over AI is that it can actually function properly. Doesn’t mean people won’t try and deploy it and use it in situations. Potentially then I think there are big risks of doing that and some of these are reflected here.

Yeah. OK, so, so, so it’s that you think people will do it without thinking about the risks and we’ll certainly find that something important is depending on, you know, basically some rubbish AI, yes, yeah.

### P14: Somewhat agree

### P15: No opinion

### P16: Somewhat agree

Yeah, because again, same with OT. You know it’s gonna be developed by very sophisticated attackers, nation States and a handful of them that have the ability to so poisoning AI is very easy, but poisoning AI to get the AI to deliver an outcome that you can control. It’s much more complicated because just like we said, you know, AI is a black box. So so poisoning. Yes. But to do what exactly?

That’s the tricky part.

So, so, so poison.

To render the AI inoperative, that’s one thing, but poison to do to get the AI to do something on your behalf without the legitimate operator noticing. That’s an entirely different game.

And so, you know, I think it’s going to be restricted to really cutting edge attackers.

### P17: Somewhat agree

### P18: Somewhat agree

So I I’m agreeing with that one.

Somewhat agreeing towards it’s cybersecurity will tamper. Sorry cyber attackers will tamper with data sets using to train AMR US causing instance directly. Or yeah, no, I agree with that.

### P19: Somewhat agree

### P20: Strongly agree

Just on reception that I would put that in that category, I think this is going to be poison of AI is going to become a bigger problem.

### P21: Somewhat agree

### P22: Somewhat agree

### P23: Somewhat agree

### P24: Somewhat agree

OK. Yeah, well it’s it’s similar to like the for me the like the previous attacks. So I would.

Classify them or rate them with the same. Somewhat agree.

## Question: AI-based phishing, whaling and similar attacks

**Description**: Towards 2040, generative AI will be widely used in fraudulent communication, by video, email and voice, leading to damaging incidents, the installation of malware, and other issues.

Totals

No Opinion: 4

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 5

Strongly agree: 11

### P3: No opinion

### P4: Somewhat disagree

### P5: No opinion

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

### P9: Somewhat agree

### P10: Strongly agree

### P11: Strongly agree

### P12: Strongly agree

### P13: Strongly agree

### P14: No opinion

### P15: No opinion

### P16: Strongly agree

### P17: Somewhat agree

### P18: Strongly agree

### P19: Somewhat agree

### P20: Strongly agree

Fishing whaling.

Yes, I would agree with that. That AI based fishing whaling and similar attacks will.

Be widely used. ~~Unfortunate~~ in fraudulent communication.

Definitely.

Increasing usage of cyber attackers we use in terms of our system. Yeah, yes, I think that that’s undoubtedly true.

### P21: Somewhat agree

### P22: Somewhat disagree

### P23: Strongly agree

### P24: Somewhat agree

## Question: AI identifying vulnerabilities in software

**Description**: Towards 2040, cyberattackers will increasingly use AI to find new vulnerabilities in standard software components or in systems accessible on the web, allowing them access to secure systems.

Totals

No Opinion: 2

Strongly disagree: 0

Somewhat disagree: 1

Somewhat agree: 7

Strongly agree: 12

### P3: Somewhat agree

### P4: Somewhat agree

### P5: No opinion

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

I think they will use it. They may not be successful because I feel like an artificial intelligence will not be able to find all the vulnerabilities. I don't think it's that advanced, but then again, it might be by 2040. So by 2040, yes.

### P9: Somewhat agree

### P10: Strongly agree

### P11: Strongly agree

### P12: Strongly agree

AI to identify vulnerabilities. I \*\*\*\*\*\*\* hope so.

### P13: Strongly agree

### P14: Somewhat agree

### P15: No opinion

### P16: Strongly agree

### P17: Somewhat agree

I've seen a massive rise in AI identifying vulnerabilities in software. So yeah, I've seen a lot of people. I've seen a lot of people starting to. If you look at the CVE index at the moment, you know, there's obviously increases in it and I think it's proportionately down to the fact that we can now, you know, take a library or a piece of software, train it on a local language model and say, right, how do we identify vulnerability here and how do we craft a payload for that to then exploit it?

### P18: Strongly agree

### P19: Somewhat agree

### P20: Strongly agree

### P21: Strongly agree

### P22: Somewhat agree

### P23: Strongly agree

### P24: Somewhat disagree

We'll use increasing use of AI to find new vulnerabilities in.

Yeah, but at the same time.

Like the developers will also find ways to try to make it more secure. I believe, or I want to believe so. I would say like somewhat disagree.

## Question: Quantum-enabled breaking of encryption

**Description**: In the 2040 timeframe, nation states and rich corporations may be able to ‘crack’ the encryption algorithms currently in use, potentially allowing them control of sensitive installations.

Totals

No Opinion: 7

Strongly disagree: 2

Somewhat disagree: 5

Somewhat agree: 5

Strongly agree: 3

### P3: No opinion

The solutions for the quantum thing.

A commercial and technical you can do it.

Yeah, yeah. Someone just said double the length of the keys. Job done.

Yeah, I don't. That's not true. That won't work. That won't work. No, that's not the solution.

Yeah. Yeah, maybe. But yeah. But you know, we've got very, you know, there's people you know, there are algorithms that are, you know, and and sort of schemes that are quantum safe and all this kind of stuff. The issue really is going to be around how do we move that out and all that kind of stuff. So that's that's why. But I think it's a game, Jake. You know, if it comes off, it's a game changer and it's going to be massive and for CNI because of all these legacy systems.

Right. We. Yeah, there's there's a. There's a huge risk. Is it, you know, is it going to be shortstop? I don't know. Poor response accidents or attacks. Yeah. An OT attacks. Yeah. I think we just felt a little bit kind of more significant than the other ones, I suppose.

### P4: Strongly disagree

Quantum enabled breaking of encryption nation states will be able to crack the encryption currently use, allowing them. Yeah, because I think what will? Because I think post Con advanced in post quantum crypto I think are such that.

They will. I I would assume or hope that by then the key exchange or the key establishment protocols will be post quantum.

Yeah, even if it's just I was. I was amused when he said, oh, just double the key length. Yes. Yeah. Yes, yes, yes.

No, no, no. Well, that is, that is the mitigation because the quantum algorithm for dealing with with symmetrics crypto is are not are not as efficient.

So yeah, no. Well, no, but that is literally the mitigation. Double the key length until it becomes until you need stronger quantum computers that literally aren't, aren't they? I mean, what are they factoring at the moment it 14 or 15 or something?

It's it's gonna have to come a long way. I mean, even even asymmetric crypto is going to have to come a long way.

### P5: No opinion

### P6: Strongly agree

### P7: Strongly agree

### P8: No opinion

You know why I don't want to give an opinion about this one because a lot of these things need to have a motivation. I don't think from the human side the motivation there yet.

Where’s the ~~There's a~~ motivation. It comes with a lot of risk as well, so therefore I I I disagree actually with this, but I'm just leaving because I don't know which state so I can go from country to country.

### P9: Somewhat agree

### P10: Somewhat disagree

no, quantum is not going to be the big, you know, deal breaker really. And then suddenly was feeling really strongly about and you know a number of things. I haven't had coffee or anything but this is not chemically induced change of mind. I was really I was sort of surprised at myself that that those were my feelings.

Right. That's exactly. I think it's going to change the world, but not in that time frame, not 2014. Yeah, yeah.

### P11: Somewhat agree

### P12: No opinion

And quantum enabled. Breakthrough. Yeah, I again. I I kind of somewhat disagree. I don't want to be super pessimistic about quantum computing, but, like, you know, show me the money.

### P13: Strongly disagree

### P14: No opinion

### P15: No opinion

### P16: Somewhat agree

OK so so I'm slightly more so you see the difference here with the previous.

Question on on quantum. So the the, the general question I say well disruption, you know all of that. I'm I'm not so sure for this. I'm a bit more confident because I think that's the perfect application of quantum.

The quantum.

Capacities that we are currently developing. So I think that might happen.

But again.

It it might even already have happened. We don't actually know, so maybe some.

The country can have.

Developed that capacity and we don't know about it and if it has happened, this country will protect that secret to the highest, you know, extent possible.

But somewhat at the same time, I've read a couple of papers where some researchers and game theory people say no. If this happens, we will know because there are enough people on the surface of the earth working on quantum to to have a hint.

But something is a fruit, and that something is happening.

But I don't know.

### P17: Somewhat disagree

And the final one is quantum on the risks.

You're you're in the, so you're you. You suspect they won't be able to crack them in that sort of time frame.

No, 'cause, I don't think there's. So it's only been in the last year or so that you can sort of rent quantum based machines and yes, they are quite capable of breaking cryptographic solutions.

You still need to have the intelligence and the research and then you've got to then basically adopt that into a proof of concept and make it commercially viable. So it's a bit like everything's vulnerable, right? Everything has a vulnerability because it's inherently got design flaws.

Just by the nature of a design, so I think you could argue that yes, it is. It is possible, but I think it requires quite a an extensive time frame to realistically.

Crack all the algorithms in use. So for example some of the elliptic curve cryptography is is kind of resistant at the moment that we know of. That may not be true in five years time, but then in five years time, you know it may be just kind of this concepts or research papers that suggest it.

There's a very different reality of converting that research into what actually I can just execute this payload that will grab some data that's encrypted with this cryptographic algorithm. And, you know, being able to decrypt it and get the clear text from it. I think it's it's still quite difficult to do that. I don't think it's possible. I don't think it'll happen in 20 by 2014.

### P18: Strongly agree

### P19: Somewhat disagree

### P20: Somewhat agree

2040 yeah, I think again, there's a debate wider debate about when we're going to get to, you know, these more advanced quantum systems. So I'll put some for that.

### P21: No opinion

### P22: Somewhat disagree

### P23: Somewhat disagree

### P24: Somewhat agree

# MITIGATIONS

**Description:** General Comments about Risk Mitigation Strategies,

<Files\\P14R2> - § 2 references coded [1.63% Coverage]

I mean, frankly, this set.

You could argue that every every one of them is is relevant and the only ones I I I disagree with is where frankly all of them are worthy. But it would be the detail would probably emerge once you were doing some of the risk management.

OK, but well, the trouble with this whole page then is there's a lot of motherhood and apple pie 'cause you could strongly agree with absolutely everything.

And it it might have been helpful if you'd said if you invited people to prioritise or order.

Force us to say which are the ones we should.

<Files\\P15R2> - § 6 references coded [4.07% Coverage]

Oh, also just in terms of if you're looking to group them, it seemed to be that 3/5 and six were all about people you'd like. People using the technology.

I increased digitisation in end users depend on it more to do things and system operators will be interacting with that in a different way. So I thought it might be more useful to put them together and also just change the order which would be 365.

Oh yeah, just just obey in my bonnet with my current climate change adaptation. People are obsessed by mitigation and actually from the perspective of risks, you would probably be better off thinking about ~~mitigate~~ adaptation, not mitigation.

Sexy technical systems and how they're acting, so I was wondering whether there might be a way that you could use that to order things because we hop around from attack, attack issue, things are linked.

So if you can go up, I think like your sort of comments, again, I think you've got about resilience. You've got a couple of things about research. They are probably group them together. But if you're going to make, if you're going to suggest about like a solution would be research into sociotechnical approaches, well, the shed loads of them already.

Like so. So what is it like? Is there a particular gap or a particular question that you think research enters? Is it sociotechnical when also what does the word approach mean in this particular like?

Approach to what like?

Approach to managing risk approach to to making products approach to running a CNI site or some C and I infrastructure.

Are we only looking at security because you mentioned security, but there's a whole lot of other things that could could be researched relating to the interaction between those like human social aspects and processes and physical infrastructures and digital infrastructures.

And and yet that you do give one specific example, but I think that's perhaps too specific and doesn't sort of encompass the different aspects that that your research probably has looked into.

So then 15 and 13 and the earlier point are all about research, so probably just have a point saying how can we, how can research better inform this thing. And then you just have three points underneath it.

<Files\\P16R2> - § 4 references coded [2.52% Coverage]

Yes, I agreed with most of the most of the statements. And again, as I said, yeah, I mean it in in the sense that I think that all of it is is needed and so we need so, so and somewhat agree we're very weak kind of deviations from the strongly agree in the sense that maybe you know less.

Priority, you know, less of a priority, but still important in the sense that we want.

I mean, we we won't be able to tackle all of those in the with the same level of intensity, so somewhat agreed. Say, OK. Well, maybe that's important, but.

Let's focus on on focus on on more kind of priority outcomes or activities first.

<Files\\P17R2> - § 3 references coded [2.78% Coverage]

Yeah, I think so. If I, if I look at them individually, I think it's a combination of all of them, which is what I feel is needed in order to quantify what's what's actually required. So yes, systems resilient approach is needed, but at the same time, I think all the other controls, it is not an individual control. If I look at an individual, I'm like, no, I disagree. It's a collective across all of them. It has to be a holistic approach. And I tell you why.

The big bugbear of mine, and I'll tell you why I often deal. Well, I try and deal with new clients where I'm like, oh, we we can offer something or, you know, have you considered having this which will help you do a little bit of identify and protect if you think about the NIST life cycle, I try and sort of break it into stages so people understand that it's covering this quadrant and that quadrant, but not all of them. And I often get told, you know, well, no, we've got this. We've got this solution. So we don't need cyber or we don't need any cybersecurity because we're covered by one solution.

And I'm a bit like. OK, well, you realise there's a whole Bank of different controls which are very different to each other than all complement each other, but not one control or a group of controls will give you complete, you know, defence in depth and protection. You've got to think quite dispersable, you know, you've got to be quite quantitive about it. And yes, in a reality, you're not going to have every single control at a very high maturity level that you've pretty much got the, you know, the whole Grapevine ticked off. And that's my biggest Bubba, if I look at them single single individually, which is what my clients, that the clients I want to work with do that.

And I'm like, no, no, no. You need to be looking at this, this and this. And I'm not asking you to look at all of them, but I think you need to have a quantitative distribution across the control array to say that you're in a relatively good shape to defend, to identify, detect, identify and protect yourself, but then have the ability to detect, respond and recover from attacks as well. So that's why I sort of was like, yeah, I can't. I can't agree with any of them until it's collectively. So that's that's why all of them.

<Files\\P22R2> - § 1 reference coded [1.77% Coverage]

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.

## Question: Systems Resilience approach

**Description**: Designing and organising to provide resilience (in addition to cybersecurity), such as incident planning, redundancy in provision, and gradual degradation.

Totals

No Opinion: 1

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 2

Strongly agree: 16

### P3: Strongly agree

I have to have to tell you that, but I I kind of do fundamentally.

Again. Or maybe I'm going to contradict myself, but I think the way things are going.

You know, because of this complexity.

Potential complexity of systems.

Maybe the you know the nature of adversary I we need to focus on resilience as a you know, we need to resilience has to be a key property of these systems, right.

Yeah, social, social, textual properties. I think, again, maybe we've linked that to the to the resilience.

### P4: Somewhat agree

No, no, I think it's the big because I think there is still.

Again, resilience approaches are not new.

And I think that tells me is that they will be is that they will be effective.

But I think they're still some way to go before.

Uh, before they will step up. Given all these advances as well that that, that you talk about?

A lot of people are thinking about resilience. A lot of people are thinking about socio technical approaches. I mean socio technical approaches is very, I mean when I started I, I mean I was looking at security culture in 2008, no one really cared about it very much. Then there are few researchers in South Africa that published, but people, the attitude was, you know, what's the point?

Now everyone, everyone is looking at it. If only I just done it a generation later.

### P5: Strongly agree

I'm gonna say slightly agree. Everybody knows we should be doing this, but it's not happening nearly as fast as it should.

That's my input.

### P6: Strongly agree

### P7: Strongly agree

### P8: Somewhat agree

### P9: Strongly agree

And then when we do a systems resilience approach, several people have responded. But what sort of which resilience approach do you have any kind of keywords or or describers that you you would use with the you know the particular sorts of resilience approaches you you would use?

Yeah, I red. Red Teaming is a really important one. I think it's the. It's the polite word for it.

I I go and find a chap I know called xxx and I say take that down and he comes back with 100 page book that says here's 1000 ways in which I'd attack it and you can't defend against them. I win.

You know you you find someone who used to work for special forces. He used to blowing things up and say, what should I blow up? And you're gonna put it in. I so I think.

Systems thinking systems engineering.

And adversarial red teaming are are things that I would start with and some of that is about, you know, imagine you're imagine you're somebody attacking it, but you also just need to do the straightforward design. Red teaming, your your job is to defend the design that's on the table. Your job is to find to, to convince them is absolutely wrong from beginning to end. Have at it and take things apart.

And then there are there are sort of. There are then some design.

That's that's a resilience testing, if you like, but there are some design ideas that can go in there. Decoupling error detection and correction.

A graceful failure.

Duplication. All these sorts of diversification, all these sorts of sorts of things. There are. There are complex systems that create a fragile condition. There are complexities that create anti fragile conditions and there are reasonably well understood patterns that lead to the one rather than the other. So we should seek those.

Make it like the NHS. Put it, put it at the edge of chaos and it'll survive anything, including having a budget cut.

### P10: Strongly agree

### P11: Strongly agree

Well, so there's a there's a kind of pseudo academic answer to start with, which is that resilience has two aspects to it. It's the the resistance to the perturbation and the restitution to status quo ante or maybe not status quo auntie, but a new acceptable state, a new acceptable state.

So does that you know the resistance and then the the elasticity into you can regard it as being the effects of elasticity in both cases?

So you then say resilience to what I would say the.

One of the observations about.

Cyber attacks against complex systems is you can't actually tell whether it was a cyber attack or.

An emergent fault of some description. In other words, the state's machine, the the.

There's the complex machine has gone into a state that was not as designed.

It's very difficult to distinguish between those and therefore resilience needs to be seen.

In the context of both of them, if we need to design our system so that they're resilient to perturbation outside their design envelope, either due to user error complex.

Often driven by poor user requirements, for example, or poor requirements, management and expression, or malicious action, and the fact is that the systems are now too complex for us to be able to distinguish the root cause.

A lot of forensic work, so we shouldn't predicate our response on it being.

On identifying malicious action, I think this is a short in the decades viewpoint, this is a short term approach that won't ultimately won't actually help.

It won't get us to where we need to be. There's.

Well, the separation of cyber against attack, against accident, against whatever is is arbitrary. Yes, yeah.

Yes, I I think that it is increasingly spurious.

There you go. There you go. There you go. And that's what occurred to me. That's what you were talking about here. That's that's the supply chain issue. It's the resilience issue. It's the failure to be able to observe. We we can't observe our system. In other words, nobody's sitting on the top of that big pile of stuff can see far enough down to realise that we're all reliant on some bit of code somewhere that runs network. I don't know what it ran some network.

Well, how? How? How could we build a system in all conscience? How could we find ourselves in this situation? And then people say, well, the solution to this is that we we run around looking at CV scores.

We're starting in the wrong place. That's why I put system resilience and secure by design, training of professionals, improved risk management and et cetera further up and stuff like research and sociotechnical errors.

An IA I'm sorry, AI incident prediction. They have a role.

Not if you're trying to defend the CNI.

In the long term.

Yes, I'm a stop and move on.

### P12: Strongly agree

Yeah. System diversity. Yeah, systems diversity and systems resilience are hard because I guess I see one as a means to the other, but I'll put systems resilience because I don't want to commit to systems diversity being the solution, even though I personally think it is.

Yeah. And also like physical infrastructure resilience. I mean, one of the reasons why I think you know this is again me acknowledging my myopia bias. But I I think one of the reasons why I want to believe in systems resilience is that it's something that antitrust action can help with, like by trust busting data. You know, we actively create systems diversity and I think that's where I'm, you know, so but again, it's like one of those things where it needs like an X-Files, I want to believe you.

### P13: Strongly agree

### P14: Strongly agree

If people have been taking the sorts of actions we're recommending to increased resilience and reduce vulnerability, then it's not such a big deal.

### P15: No opinion

There are so many definitions of resilience out there - it would be helpful to specify what exactly you mean for the purposes of this research. There is no right r wrong answer, but the reader needs to know what lens of resilience you mean - in particular because different groups view resilience as different things and you might be speaking to multiple professional audiences who have a differrent perspective on what you mean therefore understand things in a different way.

Also - specify what you mean by a systems approach - e.g. thinking about how different parts of the system come together at different times - rather than looking at things as an isolated mini system in a bigger network of systems.

ANT (Actor Network Theory) is a helpful way of looking at this - every time you pick a scale of a ‘system’ that you want to look at, it is made up of loads of tiny smaller systems of things working together, and equally is part of a bigger group of things working together as a system at a bigger scale.

Oh yeah, this is my port. My point of resilience. Like what? What are you talking about? With resilience? Like, there's like a million different like histories of resilience. What are you like? And you can get easily get bogged down in a what is the definition? There is no the definition. Just choose one and be clear when you're saying that a systems resilience approach would help manage these risks.

What do you actually mean when you say that? And how does that differentiate from from anything else that they might otherwise be doing? Because these sites will all have a resilience approach. I would argue that like traditionally Emergency Management hasn't hasn't taken a systems approach to looking at things. Security would look at security issues, safety would look at safety issues, emergency planning would write a plan that related to this kind of incident, but wouldn't necessarily like the risk management process wouldn't necessarily inform which things they're focusing and planning for.

As as in it depends like some industries would do, but not necessarily all, but the sort of assistant and I would argue that for emergency planners resilience like taking a resilience approach is about systems thinking. And it is about thinking about how all of these different things fit together and not just this one thing in isolation or as a business continuity of this service because.

Like all of these things linked together, as we keep on saying.

So you need to understand how all of those things link together and and therefore the cascading effect of you've got a problem over here, which is fine, and after two days it is going to cause another problem over here and this might be a relatively minor thing, but it will come back and bite you over here. So you think of all altogether and then over a different time frame.

And then just, yeah, I made the point about actor network theory being kind of, it could be a useful.

Way of talking about this system of systems.

It's it's just how you're talking about these things. So we we talk about things in indistinct categories as if they sit on their own, but they don't.

Focus. But you for the purpose of that conversation tend to cut it off from everything, as if it sits on its own, where is actually like when you reintroduce it does sit in within a wider.

### P16: Strongly agree

Again, resilience. I'm I'm a big I'm. I'm very big on resilience. So because I think attacks, you know that's the step and and and it it also explains a lot of my answers you know we will not be able to deflect all of the attacks but if we know how to respond and how to recover.

Quickly, then those attacks, consequences will not be that severe and we'll be able to to live with them or to tolerate them a lot more. A lot better.

### P17: Somewhat disagree

So yes, systems resilient approach is needed, but at the same time, I think all the other controls, it is not an individual control. If I look at an individual, I'm like, no, I disagree. It's a collective across all of them.

Yeah, I did sticks. I think it was, which was, there's some resilience approach is is my golden one.

### P18: Strongly agree

So the where I've where I've put strongly agree it's having a direct impact on increasing resilience.

That that, their actions that are directly in improving the situation research if it's implemented would improve, but in its own right wound.

Does that make sense?

### P19: Strongly agree

### P20: Strongly agree

You know, resilience is is, you know, there's a whole big literature on resilience. I'm not a massive fan of the the concept, but it's important

### P21: Strongly agree

### P22: Somewhat disagree

Now, because you your background is software development.

You say, oh, designing the right sort of system is the way strokes and secure system for my design is the way to do it. Actually, if you look at what is happening, so few of the new systems are likely to be designed in the UK for a specific organisation.

And so you're looking actually at is a systems resilience approach and a secure systems by design approach built into the cloud.

What principles do they build in and what do they because people are going to use the cloud because?

They're going to.

Sense there was a whole emphasis here, missing of the fact that most people's it environment these days is the cloud.

And so systems resilience and or lack of it, secure systems by design, or lack of it is it happens in the clouds and the scope for individual infrastructure organisations.

Is in a way quite small.

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.

The answer, and I think what we're trying to do with this is articulate the question.

Because the question you started with was software risk, yes, there are those, but the way to get at them is through what they do in terms of keeping the lights on or off.

Yes

### P23: No opinion

Yeah, the IT was President Obama who made resilience, say major factor. But for government CI, so it might be that people in private CI.

Don't are less focused on it. So I would say one I agree with very strongly in part because it uses the word systems.

The the this is like the key thing is that it's a systems problem.

And we're not. We're not gonna be able to fix any of these things until we think of them in as systems problems.

So I think resilience is key because that's ultimately what we want, right? It it's like we want security even more than we want resilience even more than security.

So. So. So I think that's that's kind of like a North star.

### P24: Strongly agree

## Question: Secure systems by design

**Description**: Incorporating systems security, privacy and safety analysis—including human interaction analysis—from the earliest stages of design in creating and modifying software systems.

Totals

No Opinion: 1

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 3

Strongly agree: 15

### P3: Strongly agree

### P4: Strongly agree

### P5: Strongly agree

### P6: Strongly agree

But we, but not only for TEI, but not only for AI. Also the big momentum of open source has the same problem. It’s it’s cool. You can use libraries, your functions out there, you’re using it, there is not. So the the the innovation process is already years already. It’s dramatically increased because you can use something and immediately have a powerful function.

Now when we take now open source as an example, of course immediately we have the problem together. I think it’s a crucial one. We rely on the approach that there is a community and because it’s transparent and open, the community ensures that there are no vulnerabilities in there. There are no vectors in there. It’s designed good enough. I would say it’s an assumption, but it’s it really holds. I think we have to discuss it. I here would say.

For the moment, no opinion in between, I’m not quite sure I I have a little bit of tendency to say no, it’s not clear that really the community.

Is check is providing this high security what you’re doing when you’re writing your own code and you have some regulation in doing it so.

It is tricky at the moment. It’s even a security risk.

Potentially. Or you have a very sound, broad, real community and they can ensure it, but then you need a larger mass. And for the moment, for example, we do not. I haven’t. At least I haven’t seen. Perhaps this existing that that there is a list of open source and how large is the commune and how active is it. It should be from low, medium, high and only if it’s high you can assume OK, my assumption that the open source is usable in terms of security aspects is there.

This community Judge judgement, I don’t know. Or you again you take to roll up what also happens as a supplier, you take the open source, but now you add on additional engineering work. That means you are checking this piece of code you you create now a release management that you check it, you test it. But now you have other you need other expertise. You have to understand how to test it. How to verify it and all this stuff it’s no longer writing code.

And then you can say I put my.

Label on it as a supplier and that’s exactly now the market price, because open source was for free. But I put something around it that you can use it and that’s the reason why I have now I’m.

A commercial flavour on it and I can use it as a product, so that’s again different way of system engineering system design has to happen and happens already out there, but it’s definitely something different than just writing lines of code.

### P7: Strongly agree

### P8: Strongly agree

### P9: Somewhat agree

But it leads to a set of thinking that says I designed this component to be secure. Therefore I can use it anywhere and that undermines the first one, which is the system’s resilience. What’s secure in one context is not secure in another, and so the whole of system design, I think is more important than the component system design.

But when you do secure by design, you tend to be focusing on products, and therefore they’re sitting at that component level, not at the overall system level. So it is important, but it’s not as important as the whole of system risk appraisal to me.

### P10: Strongly agree

Yeah, yeah. And education goes back to that’s essentially, yeah, I mean, without that nothing. Right. Yeah. And then I’ve put, I mean, I do think we need systems to be secured by design. I just don’t think that the cherry Morello is is that, you know, it’s it’s an old RISC 5 architecture, but it’s just no way.

See above all my chicken and egg rant, but so we do need it. But but we’re we’re nowhere near doing that appropriately. Yeah.

### P11: Strongly agree

### P12: Somewhat agree

secured by design. So look I am like kind of a truther about secure by design. Like, I definitely think that it’s important. I also think that it can be really hard to know what attacks matter at design time. So I say some would agree because obviously it’s better to do this than to not do this. But it’s not like this will solve our issues.

It’s fine to pin your career on as long as you’re humble about what you know. It can do the same way like I did my career on Leo like systems resilience, but that will not solve a lot of the sociotechnical problems we, you know, we face still important. I’m happy to make a career. You know, my one wild and precious life on it, but at the, you know, I don’t know people. It’s funny. Like, I think that the people who do design really think design can solve the world in a way where people who do like, you know, other kinds of infrastructure work, who know that like you know they can only do so much.

### P13: Strongly agree

### P14: Strongly agree

### P15: No opinion

### P16: Somewhat agree

### P17: Somewhat disagree

Secure systems buzzers by design. So as AI say, former sort of still am an architect, that that is my kind of go to title as to if anyone asks me what I do.

It’s about looking at systems and making sure there’s enough defence. There’s enough layers of defence to what we call a secure by design approach, so making sure you’ve got considerations of three or four different layers in order to make one particular vector as secure as it can be. Yes, you could go several layers, but that’s a cost implication. So what’s the the meantime to to make it an affordable mitigation and that’s that to me is what we do as a secure secure by system approach basically. So yeah.

It's Interesting. And are those liars all technical, or are they? Do they IIe human liars?

Yeah, they, they, I guess the easiest way to explain it is technology people and process if that makes sense or technology process and people if it’s probably the the right way to describe it say and it’s not a golden rule as to whether it’s to start with people first and then technology last or technology first, it is not necessarily it’s more about looking at the problem in general and saying OK Well what is what is the problem, what’s the needle focus here and what are we trying to sort of look at from that perspective and it may be that you know we just need to educate people. So it’s a policy potentially and we need to Implement that policy.

Or it could be that we need a physical technology to block this, and that’s the first point of call before we don’t think about how do we train people about looking at detection and stuff like that. So yeah.

### P18: Strongly agree

So the where I’ve where I’ve put strongly agree it’s having a direct impact on increasing resilience.

That that, their actions that are directly in improving the situation research if it’s implemented would improve, but in its own right wound.

Does that make sense?

Maybe secure by design. Should be higher.

### P19: Strongly agree

### P20: Strongly agree

You know, secure systems by design is important, but again, I’m putting it lower down because I’m sceptical as to whether it’s going to happen.

### P21: Strongly agree

Secure systems by design. That’s sort of what I’ve felt was more the the new US approach where you make it binding that things have to be secured by design. There’s a lot of UK efforts on these things as well, but it’s not quite often they are more, more voluntary than legally binding than I’d like to see.

So those I think certainly quite impactful ways to mitigate resilience as well.

### P22: Somewhat disagree

Now, because you your background is software development.

You say, oh, designing the right sort of system is the way strokes and secure system for my design is the way to do it. Actually, if you look at what is happening, so few of the new systems are likely to be designed in the UK for a specific organisation.

And so you’re looking actually at is a systems resilience approach and a secure systems by design approach built into the cloud.

What principles do they build in and what do they because people are going to use the cloud because?

They’re going to.

Sense there was a whole emphasis here, missing of the fact that most people’s it environment these days is the cloud.

And so systems resilience and or lack of it, secure systems by design, or lack of it is it happens in the clouds and the scope for individual infrastructure organisations.

Is in a way quite small.

And what there is is entirely through negotiation with suppliers rather than directly. Yes, OK, yes.

### P23: No opinion

So I think resilience is key because that's ultimately what we want, right? It it's like we want security even more than we want resilience even more than security.

when I talk to computer scientists so like.

They all tell me that number 2 is the key, and that in fact.

It is possible to write secure?

Code up to the microkernel level that’s secure through proofs like mathematical proofs and and so who tells you that it tends to be telecom lawyers, but telecom engineers who say, yeah, we built these telephone systems and you know you cannot hack them. And we can show you can’t and they’re and and so on. And but no one listens to them because they’re old, they’re fusty.

### P24: Strongly agree

## Question: Research into Sociotechnical approaches

**Description**: Research into the non-technological/human aspects of CNI system security.

Totals

No Opinion: 1

Strongly disagree: 0

Somewhat disagree: 1

Somewhat agree: 4

Strongly agree: 15

### P3: Strongly agree

Yeah, social, social, textual properties. I think, again, maybe we've linked that to the to the resilience.

Interesting. Yes. And you mentioned Solomon that, that it actually was, you know, there's this huge problem was AI suppose managerial really sociotechnical. Yes. Yes. Yeah, yeah. Yes. Yes.

Yeah, it's an organisational issue. It's an organisation. It's massive. But yeah, it's a it's an organic cultural, it's a culture, an organisational issue.

It's not a technical problem that they're dealing with really, you know.

You know I, but again, maybe there are technical problems are usually solvable.

### P4: Somewhat agree

### P5: Somewhat agree

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

### P9: Strongly agree

Yes, I think there's going to be a very real risk that we focus on the.

Infrastructure and technical design of these systems and ignore the fact that they're a human machine complex system and.

That that will screw it up.

Petcats, as we like to say, yeah.

### P10: Strongly agree

No, no, no, no, no. I'm. I'm, I'm with you. But but it's it would be remiss for us not to be doing this if we know this is the problem. We're not. Let's do the research differently or find a way to get people to, you know, to communicate that research in a more sort of, you know, effective way but not to do it seems, seems counterintuitive at this to say the least. Yeah.

Right. Yeah, yeah. And then on the other one, the mitigation approaches, naturally we have to say, research into errors and whatever. Yeah, because, because if it's the most important, then even if we only do a little bit. Yeah. By impact. Yes. Yeah.

Yes, yes, yes, we.

Yeah, exactly. Exactly. You've framed it beautifully. Yes, that that's really it. Yeah. And as I say, it might be that we need to get better at communicating. We might need. We might need some push to people. Obviously, I have a dog in this race.

But I really do think that, you know, if something isn't working, then we need to then that's also a socio technical problem, because it's the people and the seniors and the lack of investment and the fact that this space is dominated. Actually. Yes, it's a socio technical problem. It's dominated by the techies.

And when budgets are cut and when you know people are stressed, it's the first thing to go. We can, you know, let's get back to the arc. Let's architect our our way out of it. Let's you know there are technical solutions to technical problems and that's that's we're seeing that playing out in real time right now.

### P11: Strongly agree

Yes, it was just an attempt to prioritisation. I mean, sociotechnical errors are important.

Some of my best friends have worked in areas related to that.

I suppose I would prefer.

The entire design, the entire system is seen as including the sociotechnical bits rather than just the hard technology.

Research into the socio technical areas is sort of a bit is is a part of it, but but a larger.

Part I think.

Understanding how to build systems which are easier to use the right way and harder to use the wrong way.

And that's more to do with design of the system that involves the human.

This felt this felt more like a like a bid for research.

### P12: Strongly agree

### P13: Strongly agree

### P14: Strongly agree

### P15: No opinion

And of CNI system operation - you have noted earlier that risks emerge not just from malicious intent but by ‘accident’

Well, it's the example. You basically said to say you get, you say research into social, technical, technological or sociotechnical approaches, which is a bit both a bit vague in that sense because it's it's not. Forgive me for saying it's neither use nor ornament. And then you say specifically research into non-technical slash human aspects of CNI system security. Well are you only focusing is this the CNI system security bit that I think is too specific.

Because from the conversations we've had, it's not just system security, it's CNI, like software like design, security, use interfaces with users like all sorts of like all of these aspects could be things that you were looking at the interface between those technologies, those technologies in those CNI sites with those kinds of people like in the interface of those things.

### P16: Strongly agree

### P17: Somewhat disagree

### P18: Somewhat agree

### P19: Strongly agree

### P20: Strongly agree

### P21: Strongly agree

### P22: Somewhat agree

### P23: No opinion

Well it the the problem. You know what I am worried so like my general concern there is that a lot of the a lot of like these psychological biases have just proliferated. And when you look at the underlying science.

You see, it's it. It's part of the psychology replication crisis. You know, there's 100 different new psychology biopsy psychological biases.

And they're based on experiments run on college students, and they have reproduction problems.

So I'm like, I'm sceptical. I'm I'm sceptical of this research now.

You read thinking fast and small, right? It thinking fast and slow it. It's a brilliant book. It's just brilliant. It's a Tour de force. But then when you look at the anecdotes, the anecdotes are often like to do this experiment. One day I went to the cafeteria with ketchup packets and, you know, put and and, you know, I took away all the ketchup. You know what? It's Berry kind of like from the hip. And I and now I I kind of wonder.

Like how much of this is really true.

### P24: Strongly agree

## Question: Improved risk management

**Description**: Investment in risk management: organisations identifying what can go wrong, why and how likely it is; and taking steps to mitigate each risk.

Totals

No Opinion: 2

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 6

Strongly agree: 11

### P3: Somewhat agree

Well, yeah, that’s the thing.

The sense is that I mean, this is also sort of my own frustrated efforts. I think. So I I kind of did stuff on quantitative risk management, quantitative risk assessment and stuff like that for.

Yeah, I kinda think that they’re probably pretty good at it actually as it is.

I mean, we can obviously we can do better, right? But I always think there’s this sort of what I kind of learn learned or what my sort of frustration or my kind of thing. I could never square off is how do you make it better in a cost effective way?

Right. You know, and it’s always that sort of resource trade off.

Right. You know, we can we can measure risk to the nth degree, but is it worth it?

You know, using sort of all sorts of fancy models and all that kind of stuff, and the answer’s already usually pretty obvious, but I don’t know, maybe my slightly cynical view that’s pops why I somewhat agree with it, I think.

### P4: Somewhat agree

Yeah, I mean it’s the, I mean, what are the conversations I’m having with folks at the moment? I mean you say my secure by design, I mean the government has secured by design principles and different department of appropriate that and ministry defence is one of them and we have our own flavour of that and risk features very, very heavily. So continue with risk, risk management. The idea that risk ownership is distributed to different roles, that’s not that’s not magic, I mean but you know risk is one of the few vehicles we have to sort of talk about resilience and risk and one of the measures we’ve got so.

We’ve we’ve made this change. Has the risk gone? Apple gone down?

If we if we press the button, can we get a sense of the risk posture that that we have now and you know the the fact that the fact it it’s a good thing?

It’s something that should be employed more widely, and we are interested in inhibitors for what is stopping us getting getting to to where we want to be. And as you see I’m I’m putting out a call on on how to actually support that from from a design perspective and.

For that reason, support for risk management isn’t really going to go away.

### P5: Strongly agree

I’m gonna say yes on the risk management because I think people should be doing that right now and they’re not very good at it.

### P6: Strongly agree

I think there are many risk management tools already out there. People are using the many organisations, even mine, are using a normal organisation I believe have huge Excel files where they write down all the potential risks and then they try and they ask somebody how much. How big is the risk that the whole development team is sitting in one plane and the plane can crash down? It’s there. What are we doing then?

Yeah, that’s enormous. Long list people are doing it. Yeah, it’s there. Whether it’s really helpful, it’s really working. I have. I have doubts. I don’t believe it really works. We’re doing it that we can that we can claim that we’re doing it. I believe so.

It’s not really.

It is something there and perhaps some organisations have then some kind of guidelines in the travel arrangements, aka it should never happen that more than one CEO is sitting in the same plane. It might be that they it’s written down.

These are very this is a very strong examples and even we can understand them and perhaps I would say the guidelines are written somewhere if the organisation isn’t really sticking to it, that’s a big question. It will be most to a high probability just ignored because it’s not really supporting the daily way of working. So if something happens and there is an emergency case and they have to travel to Brussels because.

Yeah, nobody will ask and check. Now, what’s my travel list? I cannot take the same plane. I’m I’m missing this meeting. It will not happen. It’s very difficult if you’re doing so, of course. Then immediately it might be. There are some organisations, but immediately then the way of working will just based on this example will be more complex, more expensive immediately or in a different kind of market. So the similarity similarity will be when we talk about information security. Of course, Secret Service is definitely working different than a normal company.

And a normal company, we’re discussing it right now. I’m even I’m doing with my team. It is over. It becomes overwhelming or complex, but expensive.

Would have to double my team or I have to lower my way of innovation. It doesn’t work so I always say to my team we cannot work like a Secret Service. Doesn’t doesn’t it doesn’t fit so per definition we take into account the risk, full stop and every business owner is doing this. You always have to make a balance between the real risk describing it is fine, but dealing with it I would say so after this excellent question is how is it incorporated the consequences? How how are we?

What are our counter measures? And that’s in the state of jard? I would think lost when we go, but when we take it serious and I believe one important approach should be should it can it because it’s too complex, it has to be somehow.

To support it, it has to be somehow make visible to the system architecture, to the designer, to the management level. OK, what does it mean? And then we have to do.

I’d call it a a risk management.

Process included in the system design. So but not not on a handwritten basis. That’s for me to excel, but on a tool support that I see. OK, there’s a risk it’s red, it’s yellow, it’s green. I can deal with it. And then I make decisions. And this decision of then in the system.

Implemented so for example if my take my travel example OK, if I have done a I’m using a travel arrangement reservation tool in my company. The tool tells me there is district rules out there. Are you sure that’s not a black box? But then the system can tell me. Are you sure that you want to violate it? It is a. It is even allowed to violate it. But please confirm. Think about it. Is it worthwhile?

And what I’m what I mean, there is always the the residual the rest of the risk it will be there. We will never be 100%.

But it makes more explicit and you see this example and suddenly everybody can deal with it. It’s it’s hand. You can handle it. That’s I think the critical question can the system architect the system designer, the system developer handled with it? And if you can handle with it the complexities and and what it has to do is understandable. He can do it. He will do it. And so we will increase the overall resilience, I believe so.

So let me take the other example and let me take the example. So that’s under confidentiality, OK. But no, I think every organisation has the same problem we are discussing now internally and I’m on the same process. I want to increase the information security and when we discuss and just two days ago I discussed with my assistant. So it should be now distribute our new rules for travel organisations to our employees.

And that if I’m sending this now to my 1000 people, I have a standstill. If everybody is really reading it, I don’t know 20 or 30 papers.

And at the end you are allowed to do nothing.

But it’s that’s that’s not practical then. I mean just. OK, then let’s stay at home. We we stop to work. It doesn’t work. Of course. If I now. Yeah, I have to be important. All those countries you have to take a new laptop without any information on it. You have not to use your mobile phone you have not to use any collectivity you use test and that and that.

What I said hey, we are not Secret Service. So yeah, I know. So there will be the rest risk. So that’s not that’s not it’s not feasible full stop.

But but now if we go to one step back and say we do now a kind of.

We forget that we understand this principle problem. Basically, we go back now on the working level and say that we have every year at 200 new projects. We are the on the project level and we start to work in a permanent process. For example what I’m doing.

A project level designing and discussing per definition in a team. OK, what’s the security level? What are the security mechanisms for this project?

And then we make decisions and then that we have a system, our project management tools, our contract tool. So for example I and my laptop, I have to think about it. I do not want and I have no critical documents and information on my laptop. I’m not interested in it because I cannot read it. Anyhow, it’s not part of my business process job on my daily basis. So per definition, so all those projects and documents which we claim beforehand.

Which are critical information pieces. I do not want to see them. I do not want to have it in my IT system. So if I use my laptop OK, you will see. Now you will find our conversation, but you don’t feed find any kind of project material of critical projects so.

In principle, we can discuss now. That’s this level when somebody steals my laptop or I’m in the in the wrong country and and the Secret Service there wants to analyse it, they get some information, but I have not.

Have now not to check what kind of information do have my laptop and so per design I have lowered the information risk. There is still something there. So if I’m now after decision or careful.

I have to travel to Iran that will be now my management decision. OK, that’s even now one step further. But that’s not all. The countries in the world. It’s only one or two. We have system now. I will say go to my it temp. Give me now a new empty laptop. I take extra process cost effort. I’m decreasing my ability to work then on a remote basis.

OK, but that’s an explicit decision. Not on everything in every country outside Europe, but on specifics. So it’s a it’s a possibility. This example now gave me the possibility now to make decisions on the fly selective one and to a permanent at the at the end to risk management and risk decision, not in principle. But I think this goes down now from system design architecture.

Yeah, the overall a big Ital system then even an architecture level and use of larger than a highmam, yeah, higher level on a on a principal level than on the on the code generation. OK, which kind of codes that I can use easy tools that innovation which kind of tests I have then to include for specific building blocks because they are more

### P7: Strongly agree

### P8: Somewhat agree

Investment in this management organisation identifies can go wrong when I’m like it.

Improved risk management.

Investment in risk management can go around. How money.

Good luck with it. I will say this is very time consuming and this is very unreliable. I don’t know how what to say.

Somewhat, I believe somewhat. I disagree. But like, like I did risk management, it doesn’t work like this. John, you can’t go one by one. I mean, how long is a lot of time consuming and you can’t predict everything.

### P9: Somewhat agree

How much I wanted to push it, but yeah, we talked a bit about the complexities of risk management, why I think it needs to to happen. I think we’ve got a lot of work to do there.

Ogc was trying to teach us how to do risk management, and he said there are civil services got a reputation for being risk averse. That’s not the case. The civil service is risk ignorant. It takes risks that no commercial organisation would ever take because the commercial organisation would do the sums and work out the numbers. The civil service doesn’t have the discipline to do that, so it does some things that are utterly stupid and some things it runs a mile from that would be really good bets. You just don’t do the logic. And I thought it was really cool, really cool. Now I’m working in the private sector. I look around and go.

I think that’s true in the private sector as well. I think the private sector gets risk lucky.

More than anything else, there are certain areas around proper engineering where you get to do risk management, but commercial risk management is.

And sacrificing chickens as far as I can see.

### P10: Strongly agree

Yeah, but that would that’s genuinely my #6, yeah.

### P11: Strongly agree

### P12: No opinion

impervious management. You know, I have no opinion about this because I think.

Like looking at the financial sector, risk management is pretty mature. It’s almost like it’s everything else that needs to happen. But then again, maybe just, you know, risk management isn’t as mature as I think it is.

### P13: Strongly agree

### P14: Strongly agree

### P15: No opinion

They are already doing ‘risk management’ but what is needed is a better understanding and identification of new risks, as well as how those risks accumulate across an industry or sector.

### P16: Somewhat agree

### P17: Somewhat disagree

Improved risk management. Yeah, often I see risk management has been quite poor in C and I and having to educate as well

### P18: Somewhat disagree

Investments in in risk management. Again it risk investment in risk management. What do we mean by that is that is that like?

Is that actually putting things in place or is it?

Management systems for risk.

It’s because it only it only so you can you can do all the risk kind of risk assessments and stuff that you ever want, but unless you do something about it and and do and and use it to reduce the risk, then it’s not going to make make any difference and the amount of times is particularly in HSEI saw people with very good risk management processes but the risks weren’t being managed because they actually weren’t do they’re putting all this process in place.

I’m not actually doing anything about the risk.

I see. Oh, is that a common problem? Oh, yes, yes, yes.

Oh, yeah, yeah, yeah. So you end up being huge amounts of kind of paperwear.

Yeah, shelfware of loads and loads of systems, but then you go out on a construction site, you know, and someone’s working next to a an edge that’s like 10 metre drop off the edge of it without any edge protection. So.

Got it. Got it. Risk, risk management. Yeah. Yeah, yeah. So, so, so huge emphasis on actually doing something about it. Yes.

Doing something about it, yeah, yeah.

Mind you, that does have. I’m taking steps to mitigate each risk at the end, so maybe I’ll be. I’ll be being harsh there. Maybe. Maybe I should say somewhat agree with that.

Yeah, like there’s an irony there in three isn’t after what I said about risk management before.

### P19: Strongly agree

### P20: Strongly agree

### P21: Strongly agree

Risk management, I think that definitely includes the human factor.

### P22: Somewhat agree

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.

Apart

Secondly, big because we need, I mean in itself, it doesn’t solve anything, but it gives you the numbers that you need for the input to other things. Is is yours is what we’re saying, right? I see I need. I do need to get hold of xxx at some point. And clearly she’s you know, way ahead of of of me.

Well, I mean, it doesn’t take anything to be way ahead of me, but she’s she’s sort of ahead of the field on this, yes.

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.

The answer, and I think what we’re trying to do with this is articulate the question.

Because the question you started with was software risk, yes, there are those, but the way to get at them is through what they do in terms of keeping the lights on or off.

Yes

### P23: No opinion

### P24: Strongly agree

## Question: AI and new technology for incident management

**Description**: AI can help with incident planning and risk management, with training exercises; and with situational awareness.

Totals

No Opinion: 4

Strongly disagree: 0

Somewhat disagree: 1

Somewhat agree: 12

Strongly agree: 4

### P3: Somewhat agree

Yeah, exactly. I I think I agree. I think it’s probably coming, but again it’s a little bit unproven and I suppose, yeah.

### P4: Somewhat agree

### P5: No opinion

### P6: Strongly agree

### P7: Strongly agree

### P8: Somewhat agree

AI. Any technology for incident management. AI can help again disadvantage, training exercises administration. Well, somewhat a great like we talked about the training can only do so much because the people before you get you give me training yesterday I forget tomorrow.

Situation awareness is not working like this. It is not. Oh look, there’s an elephant. It doesn’t work like this. You need to change the system. You need to change the design.

~~Chinese~~ design is key here. New technology. Yes. So that’s why I said new technology because this one doesn’t have, it’s just here like an AI slash new technology and then I would say yes. So that’s why I say somewhat agree.

### P9: Somewhat agree

### P10: Somewhat agree

Yeah. No, you do. Exactly. Yeah. I mean, it’s it’s not gonna be nothing, but it’s certainly not gonna be everything. Yeah.

### P11: Somewhat agree

I’m concerned with the argument that AI will solve our problems.

Let me let me try and write. Let me try and explain it this way I’ve got.

I have a society that relies upon a set of services which are controlled by complex.

Software that I cannot fully understand because it’s old, it’s been written by, you know, people have long since moved on, et cetera, et cetera. So it’s complex, it’s obscure.

And I and the tool that I reach for is going to be a further layer of obfuscation on that because I don’t understand what my algorithm is doing.

At that level that the argument is a dangerous one because it feels like the kind of grasping at straws I would expect from a politician, which is don’t worry, the technology is going to solve this for us.

That that’s my concern. I’m not saying it won’t have a role. I’m just saying don’t allow people to think that it’s job done.

It’s not. It’s actually not addressing the central issue. It’s merely adding to it. If you’re not careful, that’s I think my real worry.

Yes, the complexity one actually I was trying to think.

Yes, there’s a. There’s a nice little Bobby cartoon that I, I I can’t bring it to mine now and I can’t find it. Ignore that. You know, there are some wonderful. There are some wonderful cartoons that quite nicely illustrate some of these these points.

I think there’s a little Bobby cartoon having said it. I can’t remember now what it what it was. Let me see if I can find it on my other machine.

Yes. And the point the point you were making was for the Little Bobby cartoon was the relying on technology to solve your problems. That one. Yes. Yeah.

Yes, it’s that I have a problem I don’t understand or I don’t. I cannot observe. I cannot see. Therefore the answer is going to be that I’m going to get another piece of technology that I can’t actually understand.

To fix it and just at that level that that paradox.

A cartoon of a structure

Description automatically generated

Now I remember what it I remember the cartoon. I remember it. It’s not a little Bobby. It is a cartoon of.

Critical infrastructure and I will see. I remember now where I got it. Anyway it it shows this great. It’s a cartoon shows this great edifice and then there’s a tiny little Lego block down. Right buried down deep.

There you go. There you go. There you go. And that’s what occurred to me. That’s what you were talking about here. That’s that’s the supply chain issue. It’s the resilience issue. It’s the failure to be able to observe. We we can’t observe our system. In other words, nobody’s sitting on the top of that big pile of stuff can see far enough down to realise that we’re all reliant on some bit of code somewhere that runs network. I don’t know what it ran some network.

### P12: No opinion

### P13: Somewhat agree

### P14: Somewhat agree

### P15: No opinion

### P16: Strongly agree

### P17: Somewhat disagree

I do. So I do think AI has a really good role in instant management. I do see a really good use case. I’ve seen some use cases where you know people have built Gen AI to sort of support playbook development or you know, I’ve got this piece of data. How do I triage it? And I think it’s a comp. There’s there’s lots of different areas. Instant management is not my favourite area in cybersecurity because quite often I’ve been in the deep end of it and it’s often been unplanned.

And so I’ve had to lead it and it’s not been my, my, my greatest foray. But regardless of that, if there’s quick ways of supporting individuals and you’ve seen use cases where Gen AI ~~couldn’t~~ could support people to code who don’t know how to write software.

So you just potentially need someone who can be able to do something you know copy text or and also I have a problem. The problem being you know and then taking a response which is a technical output. So likewise with incident management trying to explain to people about in layman’s terms what they need to be doing.

Really need to communicate with could be done using AI. Likewise a lot of instant management is workflow based, so workflow typically has a really good relationship with generative AI as well because of the the improvements there. So I think workflow management is quite an interesting one as well. So yeah, there’s definitely a lot of use cases for AI in that particular area. There are new areas but I think the ones that I’ve seen seem to be quite quite prevalent and useful. You can see benefits like real benefits today sort of thing.

### P18: Somewhat agree

### P19: Somewhat agree

### P20: Somewhat agree

Yeah, I’m gonna put the soft. Yes again. Uh, not gonna be. Uh, it’s gonna be a a part of the solution.

### P21: Somewhat agree

### P22: No opinion

### P23: No opinion

Technology for incident management, I think, makes a lot of sense when you think about what llms can do and what they cannot do. One is is 1 strength is identifying anomalous situations based on existing data ‘cause they’re ultimately statistical machines.

So even the LLM might say it might be a technology that helps you understand that you are not.

You’re ignoring part of the picture, right?

We might see some loosening right of.

Look at the Department of Defence has just released this big strategy around adopting AI everywhere, and they have a new.

Policy that came out, like literally two weeks ago.

And the idea is to kind of loosen the reins a little bit.

So that it’d be easier for DoD to procure.

So that that came out in the last month, this, this new policy. So I don’t know like, are we gonna go towards more contracting controls or not?

Yeah, 12 is a big one for me. Like, I think that like one of the one of the big problems we have to deal with is our inability to create criminal deterrence for no, for straight up criminal hacking. I’m not talking about, you know, you wrote something nasty about President Biden or or president or or Putin or something like that.

We don’t have a credible.

Criminal deterrent.

Or straight up economic hackers.

So that I think that’s.

That’s important. So human errors. Social engineering. Yeah, it’s gonna.

### P24: Strongly agree

## Question: AI for incident prediction and detection

**Description**: The combination of smart sensors, ‘digital twins’ and AI can spot trends and anomalies that human-only teams might miss.

Totals

No Opinion: 3

Strongly disagree: 0

Somewhat disagree: 1

Somewhat agree: 9

Strongly agree: 8

### P3: Strongly agree

### P4: Somewhat agree

### P5: No opinion

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

### P9: Somewhat agree

### P10: Somewhat agree

### P11: Somewhat agree

### P12: No opinion

### P13: Strongly agree

### P14: Somewhat agree

### P15: No opinion

### P16: Somewhat agree

### P17: Somewhat disagree

### P18: Strongly agree

### P19: Somewhat agree

### P20: Strongly agree

### P21: Somewhat agree

### P22: Somewhat agree

### P23: No opinion

So incident detection.

And also prediction there’s there’s actually there’s some there. There are some interesting military projects on machine learning for.

Offensive hacking and and so they’re they’re mere, they’re, you know, mere mere.

Examples of the defensive systems.

But in yeah, digital twin is as as the systems become more and more complex, the digital twin is gonna be how you model, how you understand an injection into.

Intervention. So I think these recommendations are really good.

We might see some loosening right of.

Look at the Department of Defence has just released this big strategy around adopting AI everywhere, and they have a new.

Policy that came out, like literally two weeks ago.

And the idea is to kind of loosen the reins a little bit.

So that it’d be easier for DoD to procure.

So that that came out in the last month, this, this new policy. So I don’t know like, are we gonna go towards more contracting controls or not?

Yeah, 12 is a big one for me. Like, I think that like one of the one of the big problems we have to deal with is our inability to create criminal deterrence for no, for straight up criminal hacking. I’m not talking about, you know, you wrote something nasty about President Biden or or president or or Putin or something like that.

We don’t have a credible.

Criminal deterrent.

Or straight up economic hackers.

So that I think that’s.

That’s important. So human errors. Social engineering. Yeah, it’s gonna.

### P24: Strongly agree

## Question: Systems testing including red teaming

**Description**: Testing and verification for entire systems, including human operators.

Totals

No Opinion: 1

Strongly disagree: 0

Somewhat disagree: 1

Somewhat agree: 5

Strongly agree: 14

### P3: Strongly agree

### P4: Somewhat agree

### P5: Strongly agree

I would love to do more red teaming on all of our systems.

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

### P9: Strongly agree

And then when we do a systems resilience approach, several people have responded. But what sort of which resilience approach do you have any kind of keywords or or describers that you you would use with the you know the particular sorts of resilience approaches you you would use?

Yeah, I red. Red Teaming is a really important one. I think it’s the. It’s the polite word for it.

I I go and find a chap I know xxx and I say take that down and he comes back with 100 page book that says here’s 1000 ways in which I’d attack it and you can’t defend against them. I win.

You know you you find someone who used to work for special forces. He used to blowing things up and say, what should I blow up? And you’re gonna put it in. I so I think.

Systems thinking systems engineering.

And adversarial red teaming are are things that I would start with and some of that is about, you know, imagine you’re imagine you’re somebody attacking it, but you also just need to do the straightforward design. Red teaming, I job is to defend the design that’s on the table. Your job is to find to, to convince them is absolutely wrong from beginning to end. Have at it and take things apart.

And then there are there are sort of. There are then some design.

That’s that’s a resilience testing, if you like, but there are some design ideas that can go in there. Decoupling error detection and correction.

A graceful failure.

Duplication. All these sorts of diversification, all these sorts of sorts of things. There are. There are complex systems that create a fragile condition. There are complexities that create anti fragile conditions and there are reasonably well understood patterns that lead to the one rather than the other. So we should seek those.

Make it like the NHS. Put it, put it at the edge of chaos and it’ll survive anything, including having a budget cut.

### P10: Strongly agree

### P11: Strongly agree

### P12: Somewhat agree

Test verification. I guess I somewhat agree.

OK, I somewhat agree with that one. I it’s so tough. I feel like verification hasn’t really helped yet. And then I always talk to my formal verification friends and they’re like, oh, well, now we have this new proofs.

There’s new automated prover now. Now we’re going to be able to do. It’s like, OK, well, wake me up when you’ve done it, because it’s been like, however long I’ve been in this job that formal verification hasn’t really helped that much yet.

### P13: Strongly agree

### P14: Strongly agree

### P15: No opinion

Consider using a more generic term? This is a very military term and other words could be used to explain what is being done. Also include ethical hacking?

So #7, I just have a particular. It’s probably me with my. I just have a beef with the word red teaming because it assumes people know what it means and also even if you do know what it means, it means something really specific. It’s quite a military term and I think that you’re trying to just say.

Check how your systems work and and look at them in in. Yeah, yes. And so like and also. Well, I think you do.

You’ve got training later on, but like this could come under training like system like testing and exercising both the systems and the operators and trying to do things like ethical hacking. So I’d say that would only be 1 aspect of it because again that assumes malicious intent and if we’ve just said that some of the risks are not malicious intent, then we need to see the other ways in which make in which they might fall apart by somebody not being able to see a flashing red light on one screen when they’re operating in another room kind of thing.

So just expand the word to testing and exercising.

Including including ethical hacking and and trying to find weak points in in security aspects.

### P16: Somewhat agree

### P17: Somewhat disagree

### P18: Somewhat agree

### P19: Strongly agree

### P20: Strongly agree

I think they’ve got to do more work around this and I don’t think the resources are there at all, you know really to do comprehensive testing of AI systems at scale. I think this is a huge problem and I do think that the government and I do think the UK is falling behind on this.

### P21: Strongly agree

Risk management, I think that definitely includes the human factor.

As well, and then testing and red teaming that also seem to be quite a successful.

Way to prepare for our ransomware case study.

### P22: Somewhat agree

### P23: No opinion

I’d red teaming.

Yeah, yeah, it’s it’s definitely is is going to be important as well. It is a a really good recommendations.

### P24: Strongly agree

## Question: Tracking existing attacks and failures

**Description**: Legislation and systems to ensure anonymised data sharing of all commercial cyberattacks and serious software failures related to CNI.

Totals

No Opinion: 1

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 10

Strongly agree: 8

### P3: Somewhat agree

Two issues there.

I’m not sure legislation is the key.

To to enabling that.

On doing more of that.

I think you sort of have to show the benefit.

‘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.

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.

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?

Yeah, but I I, yeah. Again, I don’t think with that bad at the moment to be honest.

No, the NCSC collects this sort of stuff and probably knows a lot more than they tell us. Yes, yes.

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.

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.

### P4: Somewhat agree

### P5: Somewhat disagree

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.

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.

### P6: Strongly agree

### P7: Somewhat agree

I’ll I’ll put some would agree here because on the on the tracking existing attacks and failures.

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.

### P8: Somewhat agree

### P9: Somewhat agree

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.

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.

Does that have any name or something one can reference?

Yeah, I think it’s cool. I think it’s csex. I think it’s a cybersecurity information exchange.

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?

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.

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.

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.

### P10: Somewhat agree

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.

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.

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.

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.

### P11: Somewhat agree

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.

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.

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.

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.

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.

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?

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.

Yes, but it’s because they had loyalty to each other. The lawyers absolutely prohibited it.

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 I.

That’s my reaction.

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.

So the people who aren’t part of this just haven’t been invited.

### P12: Strongly agree

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.

### P13: Strongly agree

### P14: Strongly agree

Systems

‘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 threats they’re facing.

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.

There’s a here we are the Computer Misuse Act. 1990 is outdated. It criminalises what security teams need to do.

Following her 2018 article proposing a public interest defence to the UK Cybercrime legislation she has initiated and is actively involved in the project of reforming the UK Computer Masseuse Act 1990, coordinated by the Criminal Law Reform Network, CRLNNI don’t know why the second N comes from.

So if you were to just do a search for criminal law reform network.

I think they might even have a website and you’ll find her paper and stuff they’ve done on that.

Yeah. Yeah. So yeah. So legislation is rarely needed to help track existing attacks and failures.

### P15: No opinion

### P16: Strongly agree

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.

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.

### P17: Somewhat disagree

### P18: Somewhat agree

### P19: Strongly agree

### P20: Somewhat agree

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.

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,

### P21: Strongly agree

### P22: Strongly agree

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.

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. For maintenance.

That, but it’s absolutely true. Yeah, 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.

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.

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.

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.

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.

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.

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.

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.

Apart from anything else at the moment we don’t have a way of doing that risk assessment really.

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.

The answer, and I think what we’re trying to do with this is articulate the question.

Because

Yes. And in order to do that, you need the numbers, yes.

### P23: No opinion

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.

### P24: Somewhat agree

prediction and detection, yes.

Systems testing, yes.

Trucking existing attacks and failures.

Follow up and like lessons learned so.

## Question: Systems diversity

**Description**: Regulation and guidance to promote software (and hardware) diversity, to create resilience against vulnerabilities.

Totals

No Opinion: 3

Strongly disagree: 0

Somewhat disagree: 5

Somewhat agree: 4

Strongly agree: 9

### P3: Somewhat disagree

Yeah. I just think that's a commercial, non starter.

It's just, I just, it's just not going to happen. Yeah, it's just not going to happen. It really. I mean, there's all sorts of reasons, I mean.

Yeah, I yeah, I, I I don't see that's the way it's going commercially. I don't think there's any.

And the benefits?

Possibly limited.

### P4: Somewhat disagree

A regulation and guidance to yeah, I mean it's just some diversity is hard. I mean, how do you, I mean oddly enough, one of the things we talked about on the course yesterday is sort of how do you measure it if you're proposing it as a means for safety, how do you know if you've got diversity? I mean, you could argue as indeed I did that if you had something developed by a formal approaches and everything is mathematically specified and you've got means of verifying it, you know, you could verify 2 refinements.

To ensure that your requirements are your requirements are being verified, but there is sufficient diversity, but.

You know how often you're going to see that? Probably not very often.

I guess the fact that people use APIs to act to plug into services means that I guess for some common set of services you you already have some measure of diversity. But this we're talking about diversity as a as a resilience mechanism here.

In in lieu of hardware, but.

Yeah. I I I think this is an area where you're gonna rely more on hardware than software for the for the for the for CLI anyway.

### P5: Strongly agree

100% we should do diversity. That's what we teach.

### P6: Strongly agree

### P7: Strongly agree

### P8: Somewhat agree

regulation and guidance from our software and hardware that we should create resilience against vulnerabilities. Again, they are keeping. They keep ignoring the human side of things to create. I know they are doing it now, but I just say OK there's somehow.

### P9: Strongly agree

System systems. Yeah, I'm again. I'm not sure talking to the right. Yes, I think that's it to my mind. That's part of systems resilience. So. So you know, diversity of component and and different failure mechanisms is as much a part of.

### P10: Strongly agree

### P11: Somewhat agree

Oh, no. Regulations promote university to create resilience. It's the IT was the regulation bit.

Prefers that the designers come to the conclusion they need diversity.

Rather than us being told to do it.

To factoring resilience as part of the design which leads you to diversity, yes, see, yes, yes.

Yes, for a reason. Sufficient diversity as the need demands rather than in a rather clunky.

Yeah, chunky regulation driven manner.

Otherwise you'll end up with ridiculous rules like you can't use the same firewall within 15 metres of another firewall. You know something which makes no sense.

### P12: Strongly agree

Yeah. System diversity. Yeah, systems diversity and systems resilience are hard because I guess I see one as a means to the other, but I'll put systems resilience because I don't want to commit to systems diversity being the solution, even though I personally think it is.

I I mean preaching the choir. I I I I'm. I'm so pleased to hear that you've reached out to a diversity of people and came around that I happen to be right all along without my even having to do that.

Because I just got lucky. You know, there's no, I I did not do a rigorous, you know, necessarily so.

### P13: Somewhat agree

It's an interesting idea.

But I in commercial realm.

Well, yeah, I remember a bit been about very about in order to make system diversity work.

I mean, what you're you're really looking at is having multiple?

Systems running in parallel.

So massively costly.

And could only ever be driven, I think, by governments. I mean for a commercial.

Imperative probably probably wouldn't work, but I mean I understand why it comes on. I mean, if you look at, for example, lots of open source software that all builds off the same open source software stack, I mean.

And you detect bugs slow down in those. It affects all sorts of systems and they make them vulnerable to attack. But.

I I don't know, I mean.

### P14: No opinion

### P15: No opinion

Is this not part of point 1? Or is the point about regulation being needed?

So that was about resilience again.

See, I don't know whether your point is about. I don't know. They're kind of similar, ish. And at least related. So I think they need to be speaking to each other because actually, if your point is the fact that you need to have regulation and guidance, then you're you're sort of summary systems. Diversity doesn't speak to that. But diversity is one of the things that you mentioned in resilience in that you're not keeping all your eggs in one basket.

Them slightly. I think there are two points in there, but it's not systems diversity.

### P16: Somewhat agree

### P17: Somewhat disagree

### P18: Strongly agree

Yeah, I think that's that's.

So be very difficult to manage risks with with security very difficult to Prove software's good enough.

So having diversity, so two things can't fail the same way I think is really, really important.

So if there was strongly, strongly agree, then I'd have put it in there.

### P19: Strongly agree

### P20: Somewhat disagree

Yeah, I mean, I guess does diversity create resilience? I'm not sure that that's always the case.

You know, I've seen some research saying trends, actually we need, we need to have less diversity, we need to consolidate things and have less suppliers and less systems. So that we know what's happening with them. So there's this, there's this sort of push in the other direction. So I I I'd question that assumption perhaps.

### P21: No opinion

Yeah, I think the the intuition is yes.

But then I didn't feel like I could make a judgement because at the same time I think some things are secure because not everyone has a has their own fiddly improvised own solution for things.

Yeah. Yeah, that's it's it's easy to secure one thing then, then dozens. Yes.

Yeah. And I think as long as we do follow, so the US idea of holding large vendors more accountable ~~than~~ the Microsoft's and so on.

I kind of yeah, I just didn't quite know where I would fall balancing those two two arguments. So that's why I said no opinion.

### P22: Somewhat disagree

And what there is is entirely through negotiation with suppliers rather than directly. Yes, OK, yes.

### P23: No opinion

I don't know what's gonna happen with systems diversity. I I'm. This is. I've just noticed that that with these networked environments, you never end up with great diversity. You end up with two or three, you know, two or three competitors every time. So it's Microsoft, Apple and Unix.

And it's like that and everything I. And so I don't know how much diversity we can realistically.

### P24: Strongly agree

## Question: Education of stakeholders

**Description**: Training about the dangers of AI-enhanced ‘phishing’, and more basically, about what digitalisation means for their roles.

Totals

No Opinion: 2

Strongly disagree: 0

Somewhat disagree: 1

Somewhat agree: 6

Strongly agree: 12

### P3: Somewhat agree

### P4: Somewhat agree

Engineers of which developers are are a part of it. It's AI mean the sort of if you look at CNI, there's no one developer, you've got different areas, you've got different locuses of knowledge, as it were. Knowledge asymmetry, I think are a big problem and.

Education is, I mean, edwell's awareness, not so much because I think away in today, but education and training I think are important.

### P5: Strongly agree

Yes, absolutely. We need to educate people ~~and~~ on AI.

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

Education is not enough, so that's what I'm trying to say. You need to design good from scratch from the beginning. Education's take all the training about the dangers of AI and sufficient and mobility about for digitization means for their roles. Well, I'm not going to disagree. I'm just saying it's on the part of the study. Yeah, integration into software education and through training about, I mean, it's better than nothing, but again, not enough. I said strongly agree, but not enough. So please just knock this out.

### P9: Strongly agree

### P10: Strongly agree

### P11: Somewhat agree

Training

### P12: Somewhat agree

If education was going to help, it would have helped already. I think that like education is so important, we should be training people about fishing, but also why is fishing even possible? It's because of all of our broken authentication mechanisms. And finally, now you know, pass keys are rolling out and pass keys are great. And I think that's going to help a lot. And I think that like education is important but also design. You know, I I think that a lot of what education tries to do that's actually what like secure by design.

Should be doing is trying to teach that away. You know, it's like none of us need to get trained in. Like, I don't know, this is a bad analogy.

It's so much more into it compared to some of the other things that are on this list, and maybe it's because I've been primed so much with things that we both know I think are very important and aren't being invested in enough

### P13: Strongly agree

### P14: No opinion

### P15: No opinion

And then again on points 10 and 11, I think this is an interesting one because I think they're the same point because you're talking about people being either sort of knowing more and understanding more about things. And I gather from your word stakeholders and what you've used it for that you seem to mean like other people that we just need to tell them stuff so that they understand things better. We will educate them like and just push stuff onto them so they know what they should be doing. And then the training of professionals. Well, that's also.

People

### P16: Strongly agree

### P17: Somewhat disagree

And and funny enough education stakeholders because my biggest issue is not necessarily the technical individuals that want adoption of cybersecurity in their environment, in their CNI and so forth. It's the senior stakeholders, the senior management, the procurement, the directors, the engineering managers, it's it's that education aspect and my biggest job at the moment.

Is to be a champion of awareness to the industry and it's been able to talk to someone and like, I mean as I show the other day and there's lots of really cool bits of kit that people put on the railway for monitoring and data and you know mentions of AI have all been used as well to do lots of analysis and stuff. And I ask the questions, you know, how do you secure the communications between that device in your cloud? You're presumably using cloud and like, how do you monitor your cloud to make sure that it's not misconfigured?

You might be able to exploit it and they get blank faces at me, and that's like, yeah, it's because you've not been educated in the dangers and stuff and it's it's trying to communicate that actually, you know, the senior stakeholders are running, these businesses need to be aware of it. So it's, yeah, it probably should be #1, if I'm honest with you. But that's systems, resilient approaches, multi multimodal. So I think that's why it probably gets a higher value to me.

### P18: Somewhat agree

Direct prevention of the of the of the issues is it it's just a step towards doing that.

So training in itself isn't going to reduce the risk, so only for the people who were trained actually take that training and do something about it.

That's a lack of commercial interest.

So don't put that there is because I think that we've got.

The right legislation in place already. I'm not one for.

Personal opinion, not one for kind of having a separate bit of legislation for each issue that's there. Let's see if the current regulation and legislation allows us to manage the risks or or do they take the right courses of action rather than adding another set of rules to it. And because a lot of our regulation is goal setting and technologically ambivalent, then it it tends to work for most things.

### P19: Strongly agree

### P20: Somewhat agree

Here I mean I'll put degree. Obviously, I think it's important as an educator, but.

I don't. I'm not sure we can educate our way out of this problem because.

On its own, yeah. So that's the way I feel about it. You know, you can put in this meaning going to schools and as much as you like or a public awareness campaigns are still going to be lots of exploitable vulnerabilities. So I think it's one part of the answer but.

### P21: Strongly agree

Yeah, I also ranked it higher than the training of the professionals because I think it's.

I mean those, they kind of go hand in hand, but I think if you're a professional, you already have a good baseline understanding.

Whereas the the need to to broaden education to all towards.

All stakeholders, I think that felt quite important to me.

Yeah, I think that sort of trying to eliminate the human weakness.

### P22: Strongly agree

### P23: No opinion

### P24: Strongly agree

## Question: Training of professionals

**Description**: Integrating security and resilience into software education; improved training about software contracts.

Totals

No Opinion: 2

Strongly disagree: 0

Somewhat disagree: 2

Somewhat agree: 3

Strongly agree: 15

### P3: Somewhat agree

### P4: Strongly agree

Strongly agree for the training of professionals. I think that’s this is a big problem at the moment and I think a lot of problems will go if we had stronger square. I think a lot of problems we have on software would just go away.

Engineers of which developers are are a part of it. It’s AI mean the sort of if you look at CNI, there’s no one developer, you’ve got different areas, you’ve got different locuses of knowledge, as it were. Knowledge asymmetry, I think are a big problem and.

Education is, I mean, edwell’s awareness, not so much because I think away in today, but education and training I think are important.

### P5: Strongly agree

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

Education is not enough, so that’s what I’m trying to say. You need to design good from scratch from the beginning. Education’s take all the training about the dangers of AI and sufficient and mobility about for digitization means for their roles. Well, I’m not going to disagree. I’m just saying it’s on the part of the study. Yeah, integration into software education and through training about, I mean, it’s better than nothing, but again, not enough. I said strongly agree, but not enough. So please just knock this out.

### P9: Strongly agree

### P10: Strongly agree

### P11: Strongly agree

### P12: Strongly agree

### P13: Strongly agree

### P14: No opinion

### P15: No opinion

Which professionals? Points 10 and 11 seem to essentially be the same – you need to have a training and awareness programme for different kinds of stakeholders to cover basic awareness and more specifical professional development. At present you are just delineating that some people are ‘trained’ whereas others are ‘educated’.

Check

And then again on points 10 and 11, I think this is an interesting one because I think they’re the same point because you’re talking about people being either sort of knowing more and understanding more about things. And I gather from your word stakeholders and what you’ve used it for that you seem to mean like other people that we just need to tell them stuff so that they understand things better. We will educate them like and just push stuff onto them so they know what they should be doing. And then the training of professionals. Well, that’s also.

People being informed and educated about what to do, so I think there are two parts of the same thing because certain professionals will be stakeholders in other people’s stuff and the same way around them. Like what? What are you even classing as that?

And it just comes around to education and training for depending on what your role is. If you just are a general person operating in that place, if you’re interacting with it as a an external stakeholder, so.

### P16: Strongly agree

### P17: Somewhat disagree

### P18: Somewhat agree

Yeah. Again it. Yeah, only it it, yes, clearly it's important, but it's again, it's not direct.

Direct prevention of the of the of the issues is it it’s just a step towards doing that.

So training in itself isn’t going to reduce the risk, so only for the people who were trained actually take that training and do something about it.

That’s a lack of commercial interest.

So don’t put that there is because I think that we’ve got.

The right legislation in place already. I’m not one for.

Personal opinion, not one for kind of having a separate bit of legislation for each issue that’s there. Let’s see if the current regulation and legislation allows us to manage the risks or or do they take the right courses of action rather than adding another set of rules to it. And because a lot of our regulation is goal setting and technologically ambivalent, then it it tends to work for most things.

### P19: Strongly agree

### P20: Somewhat agree

### P21: Strongly agree

### P22: Strongly agree

### P23: No opinion

### P24: Strongly agree

## Question: Diplomacy around cyber threats

**Description**: Threat of military response to serious cyberattacks; imprisonment of hackers captured while travelling.

Totals

No Opinion: 6

Strongly disagree: 0

Somewhat disagree: 5

Somewhat agree: 6

Strongly agree: 4

### P3: No opinion

### P4: Somewhat disagree

Diplomacy around cyber I’m not convinced this is going to be very effective because it it because it hasn’t been very effective so far and people are simply not going to reveal the capability they’ve got. I I can tell you that right now.

Will not reveal what they’ve what they’ve got.

‘Cause it kind of defeats the purpose of of actually having a deterrent. If you tell people what it is,

### P5: Somewhat agree

We talk about this one too.

Threat of military response to cyberattacks.

Yeah, I think we do need to talk about it. I don’t. I wouldn’t put it on the end, but we do need to talk about what that looks like.

And we need to put a few resources towards that.

### P6: Strongly agree

### P7: No opinion

### P8: No opinion

### P9: Somewhat agree

Yeah, I mean, I’ve been involved in diplomacy around cyber threats and sharing cybersecurity information between nations and getting them on the same page, and it’s slow. It’s it’s important, I’m not sure.

So it’s the most urgent thing we have to be doing, partly, I suppose, is going we’re kind of already doing this. The hard part is what that conversation’s doing at the moment is crystallising a block structure.

Where we’re saying western Western CNI needs to be protected against the Russians and probably the Chinese as well. And maybe the Israelis and you know. And so you end up sort of basically drawing up sides and your diplomacy is actually about creating coalitions and one side against the other. So it has an adverse effect as much as it has a positive one.

### P10: Somewhat agree

No, I’m not. Despite risks hosting a big kind of cyber statecraft project, I’m really not convinced by this either.

### P11: Strongly agree

And and So what made me hesitate there is that that actually that that is that indication of what constitutes something which is just short of war. What what’s it’s below threshold. And this was another big big debate that went on in the central government 15 years ago.

And could we calibrate it? And that’s why I’ve put diplomacy quite high, because part of the answer here is to have an agreed.

To have a channel of dialogue that says.

We all live in the you have different match will look to each other. We live in the real world. Let us let us mutually calibrate what it means. If people do this kind of thing and let’s let’s agree what is not acceptable like we’re not going to attack each other’s hospitals or are we so.

### P12: No opinion

### P13: Somewhat agree

### P14: Somewhat disagree

Strategy stuff and the very last I strongly disagree around diplomacy. I just can’t. Don’t think that’s going to wash.

### P15: No opinion

Not clear what you mean with this point. And also maybe you want to be clear about the political and diplomatic activity is needed to defend against cyber threats?

I mean, I kind of understand that that is something that needs to happen, like definitely in terms of but but then you give a really specific thing about I didn’t really understand what the imprisonment of hackers captured while travelling like, do you want to catch them because then they can’t. They’re not a security threat. But like, are they? I don’t know.

### P16: Strongly agree

### P17: Somewhat disagree

and a little bit diplomacy around cyber threats, I think people are very cognizant that cyber is out there. It’s in the news and it’s on their radar.

I don’t think people are necessarily.

As Cognizant about how those threats materialise to to their particular use case, I think that’s a really key one. And again that comes back to #2, which is then educating the stakeholders and and sort of trying to explain to them this has happened and this has happened. Yes, it might have been a year ago, but it happened in this sector and it was this and this is what resulted is it in how would you feel if you had to deal with that yourself, you know? So yeah, the, the, the diplomacy around that is is quite is quite key as well.

So this is diplomacy between as it were organisations in the UK or or worldwide. So we’re not talking about threatening war when you get a nuclear, when you get a cyber attack. Yes. Yeah. OK, yeah. Yeah. OK. That that’s a that’s a good way of looking at it. And you said you’d actually done 6 so the so you believe in the next one.

### P18: No opinion

### P19: Somewhat disagree

### P20: Somewhat agree

Well, I guess when when has there been a military response to a serious cyber attacks? There’s very few circumstances where that’s where that’s happened.

You know the the the US killed an ISIS hacker. I talk about that in my course.

There’s an isolated examples.

Imprisonment of Hack hackers captured while travelling, you know? Sure.

You know, charge them and if they travel, you can extradite them so you know, I think this stuff’s important.

But again, it’s not the be all and end all you you’re not going to solve everything through diplomacy.

And there are serious barriers to ethically and international law, and you know, you, international humanitarian law as we know from Gaza, the if to be legal, the response has to be proportional how, you know, killing someone for hacking you is not proportional so.

In respect of the things that you’ve mentioned specifically there, there are limitations.

There’s a whole other bunch of diplomacy that’s more common around, like sanctions, for example.

The aren’t mentioned, but which are also important in shaping behaviour internationally. Then you know there was.

Negotiation of new treaties. There’s diplomacy around police cooperation, so there’s a whole bunch of stuff under.

There, which I’d say is important, but not the be all and end of all, so I’ll put it in that category somewhat agree as well.

### P21: Strongly agree

### P22: Somewhat disagree

### P23: No opinion

### P24: Somewhat agree

## Question: Research into sociotechnical errors

Description: Academic research into why human errors happen, and ways to mitigate social engineering.

Totals

No Opinion: 1

Strongly disagree: 0

Somewhat disagree: 1

Somewhat agree: 8

Strongly agree: 11

### P3: Strongly agree

### P4: Somewhat agree

If you tell people what it is, researchers sociotechnical errors.

Although you know I I’m I’m saying somewhat agree. Now I’m wondering if that’s if that should be disagreeing.

Because I mean, this research is happening.

Already and it’s been happening for a while, I mean.

So I guess on one hand I think the mitigations.

For around, I think research and social technical errors.

In terms of a mitigation that assumes that research is actually having impact, and quite frankly, I don’t think that research is actually having impact.

So I will, I will change the sorry.

So. So. So he was looking. So what he did is he took James Reason’s model of, you know, his Swiss cheese model and basically said that it is relevant for, for, for security.

So I think the research is useful and I think it’s if we’ve got the resource to do something and it’s not taking away from anything else, it’s good to see that that stuff done. But I’m not seeing. I’m not seeing much change, certainly around mitigating social engineering. I mean that seems to be, I mean we know already, I mean social engineer is going to try and precipitate people to, to commit mistakes, not errors.

The the, the, the, the people. So it’s it’s it’s often the the person being mitigated knows they’re doing something they would they shouldn’t normally do. So they’re committing a violation.

So, so sorry. It’s violation. Not not for the mistake. Yeah, yeah.

Yeah, it’s a violation of some protocol or other, but they do it, you know, but they and in a sense that most people’s job involves violating protocols somewhere because.

Yeah. So I mean, so we know why human errors happen already.

And we know their the relationship between errors violations and social engineering.

So if there needs to be more of it, I I think I would need to be convinced in what context?

That work needs to be done. Yeah. So. So maybe that is somewhat disagreeing, because I’m not 100% convinced of the impact that research has had so far.

### P5: Somewhat agree

Again, I think we do need to do this, but maybe not so hard as the others.

I’m always. I always have. I cringe when I think about government’s gonna do something for us. Oh, God. Sometimes they’re they’re good.

No, I think there should be some support from government to look at this resilience.

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

The other research of the why human error? Definitely, and ways to mitigate social engineering. Definitely. You need to dive deep.

To psychology and behavioural science and behavioural science, I think that we talked about it. You know, definitely there’s a support for it. I just a little commercial, digest a little commercial

### P9: Somewhat agree

Yeah, I think I think it is important. Like I say, I I wouldn’t. I wouldn’t sit there and say we’re not doing this. There’s lots to be going on.

All we really need to do is pay attention to it and design into our systems. And again, the reason it doesn’t happen is because all these systems are designed to a budget with a profit margin on top to a timescale which is unrealistic. And this is stuff that gets thrown off the raft on the way.

### P10: Strongly agree

Right. Yeah, yeah. And then on the other one, the mitigation approaches, naturally we have to say, research into errors and whatever. Yeah, because, because if it’s the most important, then even if we only do a little bit. Yeah. By impact. Yes. Yeah.

Yes, yes, yes, we.

Yeah, exactly. Exactly. You’ve framed it beautifully. Yes, that that’s really it. Yeah. And as I say, it might be that we need to get better at communicating. We might need. We might need some push to people. Obviously, I have a dog in this race.

But I really do think that, you know, if something isn’t working, then we need to then that’s also a socio technical problem, because it’s the people and the seniors and the lack of investment and the fact that this space is dominated. Actually. Yes, it’s a socio technical problem. It’s dominated by the techies.

And when budgets are cut and when you know people are stressed, it’s the first thing to go. We can, you know, let’s get back to the arc. Let’s architect our our way out of it. Let’s you know there are technical solutions to technical problems and that’s that’s we’re seeing that playing out in real time right now.

### P11: Somewhat agree

### P12: Strongly agree

### P13: Strongly agree

### P14: Somewhat agree

### P15: No opinion

Consider adding ‘Social Engineering in the context of information security’.

Also consider applying the myriad of academic work already conducted, looking at human errors in high risk critical industries – and applying them to these kinds of risks. Is there any research into cyber security that is needed with regards to CNI?

### P16: Strongly agree

### P17: Somewhat disagree

### P18: Somewhat agree

### P19: Strongly agree

### P20: Strongly agree

I mean, this is fundamental to me. It’s the behavioural aspect, so it’s about.

Understanding.

Uh.

Why human error occurs?

### P21: Strongly agree

### P22: Somewhat agree

### P23: No opinion

It’s gonna be a continued problem this this social technical errors. Did you read that article in the New York Times? I think yesterday about.

The people that like it’s it’s an article explaining how three very technically sophisticated people were subjected to major frauds from Internet enabled impersonation and so on. So.

### P24: Somewhat agree

Like yes, if it’s research and theory knows, like if people are.

More willing to learn or not like a specific a new software I think.

What actually would make a change is.

The training of professionals, the education of stakeholders instead of, of course, of course, the research gives like the input, but.

And wait. This one is research into social technical errors and there’s another one researching to social technical approaches.

Well, I would say like.

The other one.

Somehow includes this one how people approach.

May then lead to say like.

Are more prone to make mistakes or not.

## Question: Legislation and government support for resilience

**Description**: To address the ‘commercial dangers’ problems.

Totals

No Opinion: 1

Strongly disagree: 1

Somewhat disagree: 2

Somewhat agree: 1

Strongly agree: 16

### P3: Strongly agree

### P4: Somewhat disagree

Yeah, I'm a little bit ambivalent. Well, no, no, no. On, On the contrary, I think I think government supports for resilience I think is important. I think it's important and legislation is important, but.

Taxpayer can't do everything, you know? I mean, would you want to know that your tax is going towards?

Getting businesses more resilient at some point you can say, well, isn't this isn't isn't this the business's job to do that? Isn't this a cough for doing business? So I mean, there's a sense that I think a sense government has a role in kick starting stuff. So if we can see that there's very obviously an impasse and something needs to be done to actually address it. Then I think government.

Help by introducing legislation measures bringing people together. 'cause. We haven't got a particular stake in any one person. Just in the well-being of of, of, of, of the economy.

But sooner or later, it's not the government's job to to run the economy. It's it's, it's the market.

And we would have to.

The what? Well, yeah. So if there if more harm than good will will would would come from the thing 'cause remember the you know you know a bank for example is tied into you know a bank goes under a lot of people are going to lose their jobs going to have an impact on the things people are going to lose their sort of deposits that's going to have an impact on stuff.

Investors who put money into mortgages and things like that are going to so it it it's not. It's really no one's interest for banks and particularly banks jobs are.

What a bank does is business model is lending money to other people. So we win, yeah.

And this did happen. You know, a whole bunch. Remember, a whole bunch of electricity, electric electricity companies went under. You know, when when the electric rate rates went and under. But the market writes itself because, you know, the customers were moved somewhere else to an infrastructure that could actually support it. So I mean there. I mean, there are, I think, industry. I think industry networks are provide a little bit of resilience as well that will that will that will address this because I mean it's a long game and and bear in mind that you've got things like futures market.

The market went the way it is. Investors were saying we think this could actually happen and they are basically bought at the futures price anyway. So that's why you've got an entry derivatives market. I want Once Upon a time I worked at the international.

Petroleum exchange. So I have something of an understanding of energy derivatives.

### P5: Somewhat agree

### P6: Strongly agree

### P7: Strongly agree

### P8: Strongly agree

### P9: Strongly agree

### P10: Strongly agree

### P11: Strongly agree

### P12: Strongly agree

### P13: Strongly agree

### P14: Strongly agree

### P15: No opinion

You might have to be more specific about the kind of support that is needed and what the ‘commercial dangers are - why do they make adifference to resilience? This sentence could mean anything and everything. Also there is a huge programme of work going on around the UK’s resilience framework which might be worth mentioning. How can this research inform what is already taking place through that programme?

Yes, I think #14.

Wasn't really sure what it was that you are getting at and also you haven't made any mention of the national Resilience framework which might be useful to mention at this point and and if you've got these frameworks. And also I wasn't entirely sure what the commercial dangers are that you're referring to, I can imagine some of them, but I don't know. I'm I'm trying to understand what your point is about them in relation to.

### P16: Strongly agree

Legislation and government support for resilience. I think we are still legislating for security, not for resilience.

So I think so some. I think the UK is probably ahead of the of the game in terms of legislating for resilience, but it's a very isolated, I mean it's it's it's probably, I would say five years or 10 years ahead of the pack of most countries in terms of legislation for resilience.

Well, it's it's. Well, it's not kind of legislation, it's regulation for resilience.

So you know the banks.

With the programmes where they're red teaming or the regulator is red teaming.

Against banks to identify weaknesses the the requirements of telcos to be a lot more transparent about incidents.

The the the anti national anti fraud strategy where the financial institution.

So responsabilized a lot more so. So I think that all of these, you know the the regional resilience centres being implemented, all of this is enabled by legislation, but it's really regulations. But I included regulation in government support.

### P17: Somewhat disagree

### P18: Strongly disagree

### P19: Strongly agree

### P20: Strongly agree

Legislation and government to support support for resilience to address the lack of commercial interest. Yeah, I'm going to say super important.

Yeah, yeah. Government support for resilience means that you have you have to invest in testing, and you have to invest in systems resilience and security by design process. So I think again, I'm trying to look, I'm trying to identify the deep.

Problem and that that flow into the others probably and look I'm not again I think training and education is important, but it's not panacea for the the lack of all this stuff at the top. So that's kind of why I've ordered it in the way I have.

### P21: Strongly agree

### P22: Strongly agree

And so we contributed to a GSIT studies.

Which was proposing that the UK Government should set up model contracts for use with suppliers, and our reaction to that was, do you think Microsoft is going to sign up to a UK Government contract? Yeah. I mean, the contracts are the contracts are terrible. Their supply of focus.

The reason you know and I can't see that changing in the next five years, it might change by 2040, but the moment all the contracts are that way and if you want it, that's with contract.

And sheds most software suppliers have a standard contract and most procurement organisations are in no position to get that modified because they don't have the land route.

It is what it is.

Hence the emphasis.

Looking at the end result, what is failing capturing data and?

Homing in on the services that are important and the services that are failing and remedial measures on that because IT departments are stretched, they're they're going bananas and they need to know what is going to cause the headlines in the Daily Mirror as well of my research values, you should quite.

You know, you know what is OK? If it goes down.

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.

### P23: No opinion

Yeah, the legislation for resilience, I I think we have to fix. There's some incentive problems that.

Fixing the incentives will fix a lot.

### P24: Strongly agree

## Question: Business as Usual Cybersecurity Research and Practice

**Description**: Activities that are currently being strongly promoted and carried out.

Totals

No Opinion: 5

Strongly disagree: 1

Somewhat disagree: 5

Somewhat agree: 5

Strongly agree: 5

### P3: Strongly agree

### P4: Somewhat agree

### P5: Somewhat agree

### P6: No opinion

### P7: Somewhat disagree

Yeah, there's always, though a danger there that you know if you.

Continue business as usual is always is always a danger that you you you don't address the things that need to be addressed which is, which is what we're doing.

### P8: Strongly agree

### P9: Somewhat agree

### P10: Somewhat agree

I liked that I, as the kind of as a proposition and thought experiment and your formulation. I like that very much. Yeah. So I thought that was, yeah.

### P11: Somewhat agree

### P12: Strongly agree

### P13: Strongly agree

### P14: Strongly disagree

Very presuming logically, strongly disagreed with business as usual. If I was saying I strongly agree with some of the other things because we were going through some of the other things, you surely therefore aren't supporting the idea of just doing business as usual.

### P15: No opinion

### P16: Somewhat disagree

The only somewhat disagree I see was on business as usual cybersecurity research and practise.

In the sense that I I I I think that we need to.

Improve dramatically the the nature of the fun. Well, the the projects we fund.

In terms of cybersecurity research in practise.

We tend to still rely on.

Mono disciplinary efforts.

Where we get funding for computer science projects or even in computer science, you know, network security and.

Application security and this and that and I think we still fail to understand cybersecurity and cyber resilience as a system.

And.

To research a system, you need to bring together different types of expertise to understand the different level of operations of the system and the different kind of cogs that make up the system that may belong to different areas of practise. So I think if we keep on funding and I and I'm, I'm not saying governance or not, so it's disagree with the statement. I think government are.

Trying to.

Develop new funding models and funding streams for research and and practise of cybersecurity to develop these systemic.

Projects and interdisciplinary approaches. But at the moment we're still stuck in mental models that are still very dependent.

Business as usual and that's not it's not going to cut it.

But that's why I'm I'm really enthusiastic about your your work. Because I I see your project here as a as a call to arms in terms of you know business as usual. Sorry people. It's not gonna work.

### P17: Somewhat disagree

### P18: No opinion

### P19: Somewhat disagree

### P20: Somewhat disagree

Business as usual cybersecurity research, actually, they're currently being strongly promoted and carried out. Well, no, I think like someone disagree with that, we need to.

Step up all this stuff that seems to be the status quo approach, right?

If you want to do a lot more, you need a lot more resources to do a lot, a lot more and budgets are scarce and cyber is just one priority among many.

But I think if you if we just do the same amount, the problems can then get worse and worse. So yeah.

### P21: Strongly agree

### P22: No opinion

### P23: No opinion

### P24: No opinion

But would would this apply if like things are like keep business as usual if things are working for like certain components?

Or like what is good? Let's keep it how it is or what do you mean?