# CONTEXT

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

No relevant comments about the parent code.

## 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. |
| * Industry isn’t that influential - it is hard to share tacit knowledge about CNI. * Legacy systems demonstrate Little/no influence of industry innovation. * Industry is driven by innovation. Industry innovation should be promoted. * Industry Visions/innovations are derived from Government discourse. * Industry innovate in response to government prompts. Innovation -> State driven. * Industry in CNI are not innovators. Lack of accountability -> Lack of Commercial Drivers. * Innovation comes from people who understand CNI. E.g. CNI Spin Outs. * In CNI there are issues more important/essential than commercial drivers |
| Totals  No Opinion: 2  Strongly disagree: 0  Somewhat disagree: 4  Somewhat agree: 8  Strongly agree: 8 |

## 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.

|  |
| --- |
| * Longevity of Software hinders modernisation. * Software is not as hard to change as hard infrastructure. Not updating software is a choice. Reasons can be safety or other development reasons. * Longevity of Software should go first in the list. * Today there are more programming languages than we had 50 years ago, but we are still using those old languages like Cobol. Software lifespan is between 40 and 50 years. * Well-designed software can be maintained for a long period of time. * Depends on functionality, but Software, by nature, is not static. It is/should be easily updated and modified. * People are aware of vulnerabilities, so new iterations are needed to remove weaknesses. * Any type of knowledge is hard to preserve if there is not proper management change/control. |
| Totals  No Opinion: 1  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 10  Strongly agree: 9 |

## 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.

|  |
| --- |
| * Definitions of CNI vary constantly. New things are being added than taken away. * CNI is driven by issues and or events which are critical of ministers. * CNI - what we expect and rely upon and changes constantly. Currently it is network technology, in the future it could be networks information systems. * The text does not describe, explain what CNI is. The CNI description should come before discussion of technology and systems. We should also look at other countries’ descriptions. * CNI should be defined as series of interlinked functions as opposed to static sectors. * The list of sectors is not good. Organisations part of CNI supply chain are not classified as CNI but their failure can have significant impact. * CNI definition should be dynamic not static. * Debate/Conflict between how much do we include in CNI definition and the impracticality to manage, regulate, etc. wider definitions. * In the US CNI is mostly in the private sector. However the most important/dominant ones are public sector and should get more attention. |
| Totals  No Opinion: 1  Strongly disagree: 0  Somewhat disagree: 1  Somewhat agree: 10  Strongly agree: 10 |

## 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.

|  |
| --- |
| * Regulation drives, or at least guides or steers. Some operators are conservative and wait for clear signalling to invest. They do not want to move until the regulation is clear, e.g. to not waste money. * Standards are reached by Industry consensus. Some government people might participate but it is an Industry-led thing. However, regulations are needed because Industry cannot be trusted to work on its own on everything and because some agents might try to subvert the rules. * Most Industry sectors prefer to wait for government to regulate so they do not make mistakes and get penalised. An exception would be cybersecurity where they are being more proactive as they understand issues better. * Regulation is a two-way communication where government tell industry their expectations but where industry also proactively goes to the government to speak. * Sometimes standards can clash with commercial drivers/interest of stakeholders, no one wants to take the risk. Government is needed to intervene and regulate. * However more important than regulation is the nature of CNI. CNI cannot fail. Its demand is inelastic. So anything is done, at any cost, to keep it floating. Even at the expense of the stakeholders (?). * Commercial sector waits (needs?) to be regulated. CNI are almost self-regulating. They do not wait for regulation. They know what is at stake. Integrity rather than commercial interests. * Risk of regulatory Infraction is considered Top Risk. * Straightforward, formal compliance to regulation does not do much for resilience improvement. * Outcome based response to regulation - understand letter and spirit of regulation. Stay ahead of the game. * In the west not everyone understand the law and not necessarily everyone has to fulfil it. CNI is compliance-led and not as proactive as expected. * Nuclear is proactive in understanding where innovation might happen and what the regulator needs to do about it. * It varies across sectors. * CNI is fairly regulated. * Does not agree with “Only” in Only Respond to Regulation. It depends on the nature of CNI. There is security awareness and implementation of mitigations in telecommunications for example. |
| Totals  No Opinion: 2  Strongly disagree: 0  Somewhat disagree: 6  Somewhat agree: 11  Strongly agree: 3 |

# Trends

**Description:** General Comments Trends.

|  |
| --- |
| * Group and order trends. * A lot of things that do not work in the NHS are administrative systems rather than software. Also security is not good and there is lack of confidence from users. Data structures are not a big issue in the NHS. The current nuclear industry could be treated as legacy as it will be changing so much in the coming years. |

## 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.

|  |
| --- |
| * Difficult to predict what we will be talking about in 2040. Advanced can be defined differently depending on the sector. In nuclear tech from mid 90s could be considered new. In others much less, but there will always be a lag. It could be that by 2040 we are still talking about digital twins and cloud technologies but that would be because of the decisions we make now. * IoT is coming and growing, we will have to deal with it. * Definitely. We are already doing it in transport. It would be true in 2040 maybe before that. * IoT is already here. * Don’t know about Digital Twins. We need to provide examples of use in CNI. * It will increase. Not sure how much especially for traditional infrastructure where things might not be that different by 2040. |
| Totals  No Opinion: 1  Strongly disagree: 0  Somewhat disagree: 0  Somewhat agree: 6  Strongly agree: 15 |

## Question: System complexity and interconnectivity

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

|  |
| --- |
| * It would be true if we look broadly across the sectors but for certain sectors like nuclear it will not. Failures in security/safety have significant consequences. * Do not agree with “increased complexity”. Don’t think complexity will go up that much. Regulators would not accept something if they do not understand it. * Yes, and we will be more vulnerable in terms of human error and attacks. * Complexity and interconnectivity might make things easier to design and manage if we outsource it, but difficult to understand. * Systems are already complex and interconnected sociotechnical assemblages. Wording: are we suggesting things are not going now but will in 2040? Those things are already happening. Wording: Systems. We need to use the word systems to set out boundaries so we can talk about them but in reality there are no boundaries. * Complexity increases as more disciplines need to work together in areas in which they are not experts. IT and cyber working in engineering settings. Building IT systems for OT. * Yes but a lot of these risks can be avoided with proper engineering/design. * Systems that are not designed to work together form a complex system that people don’t understand. * Should not be that difficult if we put in place effective management processes. * Systems will be a bit more difficult but there will not be a huge difference. * Software dominates the reliability agenda and complexity and interconnectivity drives the agenda. |
| Totals  No Opinion: 1  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 8  Strongly agree: 11 |

## 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.

|  |
| --- |
| * Not sure if it would be software or software controlled hardware. What is the definition of software nowadays? Also, wording Systems are something different. Use “Infrastructure”? * Yes, but it is not necessarily that conclusive. Digitalization will come with increased deployment of physical systems and with new mechanisms of simplification and management. * Not an expert in these systems but I understand why CNI strategy would be to move towards more digitalisation. * Clarify what “physical space” is? The statemen suggest digitalisation is a mechanism to free space. Could be true for transport for example, but not for many others. |
| Totals  No Opinion: 1  Strongly disagree: 0  Somewhat disagree: 0  Somewhat agree: 7  Strongly agree: 14 |

## 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.

|  |
| --- |
| * Edge devices and sensors are getting smarter and smarter everyday. In terms of nuclear, though, as SMR will be a first of a kind, they are a bit defensive. * Improve wording. Yes, especially in railways. Not sure about small nuclear reactors. * Too much in the statements. Needs to be analysed in bits. Agree with dispersion of electricity but not with SNR. Don’t think decentralisation will be a consequence of remote communications and wireless. * Not sure if fragmentation/decentralisation is a good thing for CNI. Central coordination and oversight is safety critical. SNR should not be a thing. Don't think decentralisation will happen: the costs are too high, there are no incentives. It won't be aligned with commercialisation and external investment. It could happen in extreme cases like water where the government cannot allow it to fail. If it fails gov will pick up the pieces. * Not sure remote communications will enable decentralisation, particularly in nuclear. Electricity is already dispersed. Doubt things like waste management could even be decentralised. It’s too difficult to do on a small scale. * With distribution each individual asset/infrastructure/system will be less important, but collectively still important. So for risk analysis we need to understand the risk across all of them and how they function together. * On paper, architecture may seem decentralised but in reality, if we look at the providers, the systems are very centralised. It won’t be about decentralisation but consolidation of big companies like Microsoft, Amazon, etc. * Current mentality is, if we are worried about it, we centralise it. Core CNI will be centralised. Don’t think this mentality will change in 15 years (maybe in 50 years?). * NO to SNR for safety and security reasons. For others, questions need to be asked: can decentralisation be done in a safe and secure way? Is resilience considered? |
| Totals  No Opinion: 2  Strongly disagree: 1  Somewhat disagree: 4  Somewhat agree: 9  Strongly agree: 6 |

## 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.

|  |
| --- |
| * Technology is more reliable now but I wouldn’t say it has changed fundamentally the way I work. * Yes up to 2040, but afterwards we’ll have to find how to do this differently with data, etc. It will go over the roof. * Problem with "Reliance". There must be humans in the loop. Most of new software is buggy. People in the sector are to smart to hand over stuff to something they know is buggy. (Digital security by design exacerbates software issues, P10 will send Charles reading about Morello.) * Clarify who the end user is. Clarify if this is a dominant problem and peculiar to CNI. Society considers the Internet an essential service a human right. (This might be because people are too dependent on it? CLK) * We can see shifts about this socially. * We are already there. We will do it better and reliance will be the same amount. * Put this after point 6 - as 3, 6 and 5 are all about human interactions with CNI software. * We depend on technology, on data. Data is used as a point of reflection to see where we are and what we are doing. |
| Totals  No Opinion: 3  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 5  Strongly agree: 12 |

## 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.

|  |
| --- |
| * Can sort of see it coming. There is some potential for these things to happen, for political or commercial reasons. * Ultimately you're never going to be able to completely remove people. These things are not going to be completely automated. * Operators rely on analogue systems where safety is concerned, This is the mentality now. Maybe it will change in 15 years but do not see it as a trend. * Agree but in transport is behind. There is an awful lot that is not through software. * CNI value humans in the loop. The acceleration of advanced technologies, like chatgpt or transformer platforms make people more hesitant. They are prone to errors. There is uncertainty. * Put this trend together with Increased Digitisation. * Will move towards that. New generations getting into that field will have grown up with more technology than we did when we were starting out. * It’s happening now. * There will be a combination of human + machine. We will create Digital Twins and Virtual Systems but there will be some direct contact. * I talk to people who try to avoid full digitisation. * Need for human participation. It won’t be entirely automated. Letting software systems run themselves is not the proper pathway. |
| Totals  No Opinion: 2  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 11  Strongly agree: 7 |

## 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.

|  |
| --- |
| * Somewhat disagree. Geopolitics has an impact now. There will always be state/nation interests. There will not be any substantive change. * Busy question. There are different parts to it. What does “CNI to implement changes to mitigate harm” mean? What are the changes? Distributed energy generation is already happening. * Not sure about the first statement. In terms of climate change we are already doing it. We are providing requirements, planning for the future. * There is balkanisation at the level of information but not telecommunications. Telecommunications still works on the same global standards so everyone is able to interconnect to the same things. At information level, different language population get different norms and information sets. In terms of climate, CNI is already doing that. People working in CNI want to make those changes. * There is a division in the world with Russia, China and other countries on one side, with different values, e.g. protecting people by controlling the internet. CNI may become polarised if the world becomes geopolitically polarised. Do not understand the second part of the statement. * Agree with separation of internet. Not convinced with climate statement. * The world has been divided into blocks for centuries. (There is no reason for the Internet not to follow the same pattern. CLK)Do not think there will be a separation of the internet: having private spaces for CNI - General Internet. Regarding climate there will be an increase in OT infrastructure as we will need distributed systems, renewables, etc. to support greener energy. * Agree with both. Solar panels have been driven by climate change. * Climate change and green energy will drive and implement standards but not convinced that it will guarantee the mitigation of harms in the sector. It will be a factor but there are other important factors like government regulation and corporate responsibility for mitigation. * Internet segregation has been predicted for 20 years but still has not happened. |
| Totals  No Opinion: 4  Strongly disagree: 0  Somewhat disagree: 5  Somewhat agree: 10  Strongly agree: 3 |

## Question: New CNI

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

|  |
| --- |
| * We're already seeing this. We're seeing more and more movement to the cloud all the time. * We already live in that world. * Can understand that it is going to happen but do not know the timescales. * Communications and Internet related infrastructure are already CNI. * Digitisation will increase in OT: Internet to Cloud, but don’t think these systems will become CNI. No benefit in classifying too many things under CNI. * Seems to be saying that a guy from the White House said that telecoms was not in the list of most important CNI. (Bad quality audio and transcript CLK.) * There are already countries which treat the Internet as CNI, but not the US and UK. - UK has communications, not sure if Internet falls under communications. * Internet is already CNI. Nuclear will change radically, from big legacy systems to SNR. They will be more like the communications, energy and health sectors. Outsourcing and getting rid of legacy software faster is good for resilience. * Internet is already critical. |
| Totals  No Opinion: 2  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 6  Strongly agree: 12 |

## 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.

|  |
| --- |
| * Don’t see much positive use of AI now but the trend is moving towards. * Situational awareness is important for human factors. Example of robots and AI for maintenance and data collection. Add “safe” to “efficient and effective”. * There is much more to AI than ChatGPT and LLMs. There is powerful work on AI being done that we don’t see because it is doing something useful. There is potential for AI and ML to play a massive role in dealing with complex systems. * Sceptical about how much AI can contribute. AI has failed 2 times before, e.g. self-driving cars. * Not the universal solution. It can open doors but can also bring dangers in. * Include additional security risks with deep fakes. * With AI integration we are increasing the attack surface. People want to see the benefits and do not see the whole business case. Bad benefits are worse than moderate goods. * Question mark around efficiency and effectiveness but there is a strong trend towards their improvement. |
| Totals  No Opinion: 2  Strongly disagree: 1  Somewhat disagree: 1  Somewhat agree: 10  Strongly agree: 8 |

## 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.

|  |
| --- |
| * We are putting money on Quantum because there are applications for it. However it is not mature enough, not for cryptographic problems, and those problems can be solved by doubling the key size. Maybe in 20 to 30 years but don’t think even then. * 2040 is not that far down the line but we may see developments then. * Confident we are building quite big quantum computers in the near future. However, more research is needed into quantum mathematics and quantum computation rather than computers to unlock their potential. * Explain what we mean by Quantum. Is it quantum techniques for secure communication and other activities or quantum computing for resistant encryption? Both are different things, and maybe not related to the other trends. * Not quantum computing but quantum communication and sensing. * 2040 is too early for such a big challenge, to achieve any kind of scale. * Quantum will support solutions but 2040 is too early. * I would not formulate this statement with such certainty. AI took 75 to develop, since the 1950s. Following the same logic, it could take Quantum another 50 years. Although AI can help accelerate it. * Quantum won’t be around by 2040. Quantum on its own won’t solve problems but if it is combined with AI it will. * Quantum is not mature yet. It is less advanced than AI. There are difficulties in making it robust and usable. * 2040 is too early. One has to be very optimistic to thing that something useful will come up from this. * Disagree. People keep predicting Quantum will be commercial in “5 years”. They do not explain why 5 years. |
| Totals  No Opinion: 6  Strongly disagree: 0  Somewhat disagree: 9  Somewhat agree: 4  Strongly agree: 3 |

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

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

|  |
| --- |
| * CNI has higher demands and uses comparatively more expensive software than the one you can download from the App Store. Off-the-shelf is not entirely off-the-shelf, there is pre-existing hardware, firmware and board support packages. You/CNI cannot buy off-the-shelf and start using it right away. It needs to be customised. * Strongly agree. It is already happening. There are CNI vendors promoting this service paradigm and with the kinds of contracts they get they can do anything. * It will happen but we prefer systems to be designed from scratch and off-the-shelf is very problematic. Hardware and software are the biggest problems as users do not come in one box and they are changing all the time. * However we will also build systems out off-the-shelf components and then suddenly realise that 30% of the economy depends on a commercial provider. We will hope we'd built the system properly. Risks will emerge when systems never intended to be CNI become CNI and are using off-the-shelf. For systems we know will be CNI we will strengthen their off-the-shelf components. New things that we know are CNI we will build properly and will be expensive but built to the right standards. * I think like almost everything is and has always been plugging together stuff that already exists. But often I think it's the loo (Code? CLK) that you write in house that actually matters. * There will be increase in off-the-shelf but there will be some bespoke as well. For example, in defence, because of the security implications, they make their own thing to keep baddies away. * Disagree because they are already doing it. E.g. NHS uses crappy Windows software. |
| Totals  No Opinion: 3  Strongly disagree: 1  Somewhat disagree: 3  Somewhat agree: 8  Strongly agree: 7 |

# RISKS

**Description:** General comments about the risks parent code

|  |
| --- |
| * Some risks are much more likely than others. Others are highly unpredictable. We need to add Impact Likelihood to the list. * I think they're present now. I don't think they're about the future. * Classify risks as:   + Malicious and non-malicious   + New and known (with changing impact). * Pay attention to unknown risks. * We understand conventional risks. * Assessment and management of risks is complex as they depend on multiple factors. Nothing happens in isolation. |

## 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.

|  |
| --- |
| * Not enough people with the right skills. There is no direction towards development of new capabilities. We will probably get better at automation. Is it additional or different malicious activity? Worries about state aligned threat actors. * Poor response will still happen but it won’t increase exponentially. There are changes in norms, occupational health. There is much better response and security operations. * People are not trained as much as they should be. The more AI gets into society the more glitches we’ll see. * Poor response means people do not do what they are supposed to do. The problem is when attacks are so sophisticated that there is no response planned/possible. * Disagree with A. Systems do not take into account human limitations. We cannot train for everything. We cannot train for bad design. We cannot programme humans. Hackers study human psychology, more than engineers and designers do. Agree with B. and C. * Things will happen if there will be a lack of training. But, will there be lack of training? No. So A. and B are covered. People are being careful about AI at the moment -> C. * The UK is not well prepared. There is poor preparation. This comes under Resilience. * Those three things listed there could happen. * Poor response is already happening. * Pandemic disruption response shows CNI systems worked. We should pay attention to the people and resources already working on tackling this problem. We need research to measure the quality of responses. * No knowledge or intel is shared. Human factor is key. * Failures occur when systems are not designed properly. * There still a lot of poor responses but a lot of CNI are mature large companies - they are well trained to respond to accidents and attacks. * We have tons of data from attacks to train machine learning. * The statement is too catastrophic. It depends on how much we address the issues beforehand. |
| Totals  No Opinion: 3  Strongly disagree: 0  Somewhat disagree: 6  Somewhat agree: 11  Strongly agree: 2 |

## 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.

|  |
| --- |
| * Technologists shortcoming -> humans are stupid, the weakest link. Adversaries have an advantage as long as there are humans in the loop. Technologists blame users for their bad job. * Contention with the word Increasingly. Systems will evolve to adapt. * Humans are very vulnerable. In terms of cybersecurity, people put their best resources on People, rather than technology and processes. * It’s already happening. Main attacks on CNI happen through social engineering. * It's called social engineering. They are doing it very well. * We're increasing the opportunity, but we might also be increasing the resilience at the same time and therefore managing that. * The human factor is still quite a key one. * Deep Fake is a problem. There is work done on better methods for authentication and to detect falsification. |
| Totals  No Opinion: 4  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 6  Strongly agree: 10 |

## 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.

|  |
| --- |
| * The problem exists but not sure if it will be bigger in 2040. * We know where the risks are. Resilience will put this act together at some point. * Hard to decide what are the functions that are most important to protect. Chain reactions can happen from non-essential to vital aspects of a system. * We are increasing resilience to manage this. * Are trophic cascades relevant? CLK * This can be controlled in designed by not designing these systems completely open. Isolating systems avoids cascading effects. * The more things are connected through the Internet of Things the more likely we have system of systems failures and problems. * Cascading problems already exist. * Some people are developing software to try to map those dependencies. |
| Totals  No Opinion: 2  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 6  Strongly agree: 12 | |

## 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.

|  |
| --- |
| * Re SC: Nuclear isn't mature, banking, finance are much better. There are people doing SC mapping, understanding critical suppliers (tier 1, tier 2....), the challenges they face, and understanding who owns the problem. They would like this to become business as usual. The SC issue is not a technical but an organisational and cultural challenge with possible some technical solutions to support them. * Things will get better rather than worse. From a market perspective, healthy, robust SC are important because they give us competitive advantage a nation. Anything that gets on the way should be investigated. * SC is an issue now. Hopefully it will get better in 15y as a lot of people are working on it. * Problem is the international aspect of the SC, particularly for low level devices and services. We are not sure of our SC is UK based. * We're seeing that being beefed up. * SC are comprised of developers, software, users, data centres, all of them are different. This makes SC complex and subject to vulnerabilities. * It's about procurement and technical specialists. * SC can be scary. We cannot trust some suppliers. |
| Totals  No Opinion: 3  Strongly disagree: 1  Somewhat disagree: 3  Somewhat agree: 7  Strongly agree: 8 |

## 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.

|  |
| --- |
| * Electricity failure wouldn’t be so disruptive. There are backups for these things. * We are highly dependent on electricity, telecommunications and the internet. * If we didn't do anything about it, this would definitely be a big risk. * CNI can only function at best for a limited timeframe without those things. This is a current risk it is not something new. * Operators know the structure is fragile but they make efforts to adapt, to shift resources quickly. * We have identified risks. These systems should be safety critical with enough redundancy. * Electricity systems are easy to disrupt. * It depends whether contingencies and resilience are built into the system. Electricity systems are designed with resilience in mind. * Agree but I talk to people who are working on more independence from these things and resilience. * Too many systems rely on electricity and we do not have enough generators. Even generators can only provide a few minutes help. * Electricity failing is an example of a cascading problem. |
| Totals  No Opinion: 2  Strongly disagree: 0  Somewhat disagree: 5  Somewhat agree: 5  Strongly agree: 10 |

## 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).

|  |
| --- |
| * It is a risk but it’s disruptions rather than accidents. Maintain skilled workforce to handle these issues. * We already live in a complex world of systems. Don’t think complexity is to blame for increase in accidents. * There is also organisational and job design factors. There is good faith in systems but also in other humans. We should look into this sector by sector. * We're increasing the opportunity, but we might also be increasing the resilience at the same time and therefore managing that. * Yes, sociotechnical is important but it is probably at the bottom of the list. This is from a strategic and political point of view. * Almost everyone works in good faith. * Disagree. Optimistic that people understand the risks and design the systems appropriately without increasing complexity beyond our capabilities to understand it. * It’s already happening but don’t know if it is going up or down. * No opinion but do not agree with “all participants working in good faith”. There can be malicious activity, but also people who are doing the wrong thing because it is not possible to do the right thing. E.g. when protocols are contradictory. * Sociotechnical problems are evident issue are the more common forms of attack. * Issue isn't necessarily attacks but about social engineering. * Incidents like Mile Island and Chernobyl are good examples of why to implement security operations. Not sure if increase if interconnectivity is the source of the risk. * Not sure if digitisation is the problem. |
| Totals  No Opinion: 3  Strongly disagree: 1  Somewhat disagree: 4  Somewhat agree: 6  Strongly agree: 8 | |

## 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.

|  |
| --- |
| * Back in 2010 the feeling was: why would people care? And an attacker would need advanced, non-trivial knowledge. These views have changed now. The attacks are going to be there but the actual OT software stack would take longer to be integrated and therefore still would need stronger attacks. * It’s happening now and will continue to happen. * OT attacks are an issue. * We live in that world. * It is possible, but there is mitigation: good design and being aware of types of attacks. * Sophisticated attackers like state nations are already doing it, and they will continue. Amateur hackers: maybe if they are using AI tools, but there might be other less complicated attack options like attacking companies instead. * Disagree. OT have (need to have) data diodes which are physically impossible to break. * Problem with “destroy”. Better use interrupt, disable, disrupt. * True, but launching an cyber attack on OT is not super easy. It is quite a challenge. |
| Totals  No Opinion: 3  Strongly disagree: 1  Somewhat disagree: 1  Somewhat agree: 9  Strongly agree: 8 |

## 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.

|  |
| --- |
| Phishing and whaling will be widely used in fraudulent communication. |
| Totals  No Opinion: 4  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 5  Strongly agree: 11 |

## 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.

|  |
| --- |
| * Disagree. It is a concern, but people are talking about this, thinking about strategies to sort this: resilience, diversity, monitoring. * It is easier to use the same provider for everything. Safety and security guides go for diversity of vendors but it adds cost. It is happening today and it will remain the same in 15 years. * Wouldn’t think that CNI systems are vulnerable as they are fairly bespoke . It would take a lot of effort to design an attack that cannot be replicated elsewhere. * This would be a risk if we did not do anything about it. (The real risks are the ones we don’t know about/ cannot imagine? CLK.) Common failures, cascading and complexity failures are very hard to fix because we don’t think in systems terms very often. * Disagree. It will happen but we have to consider our capacity to response and recover. * Disagree. OT markets are getting bigger with a diverse range of technologies. * Agree with everything. If you have everything with the same system everything is vulnerable to the same failure. * Yes, there are not completely bespoke systems operating across areas. Clarify: “geographically dispersed” Is it same company operating in multiple countries, or different organisations using the same technology? * The National Preparedness Commission is worried about this. * Already happening. Common failure is cascading failure. |
| Totals  No Opinion: 2  Strongly disagree: 0  Somewhat disagree: 6  Somewhat agree: 6  Strongly agree: 8 |

## 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.

|  |
| --- |
| * It is coming. For financially motivated adversaries, use of AI will only be valid if there is money. NCSC podcast about AI and adversarial use of AI: the benefits of AI for the defenders are bigger than the attackers. * There will be always people trying to take advantage from/exploit new technologies. * It’s happening now. You do not need to technical skills. You just need a credit card. * Availability of tools will not be enough. There are other factors in play: team work, social skills, so availability won’t be sufficient motivation. * Yes, democratisation of technology will increase risk. No, it will not cause damage on systems and infrastructure. We can’t allow that to happen. We have the tools to make sure it doesn’t. * Blunt AI tools will be available to enable cyber attacks by non-state actors. But massively damaging cyberattacks won’t be the case. The more advanced technologies will be in the hands of the state apparatus to counter those attacks. * There won’t be a fundamental change. AI won’t be a game changer. There is so much already available (tools and instructions) and you don’t have to be particularly skilled. * “Accidentally” relates to sociotechnical problems. “Unintentionally” rather than “accidental”. |
| Totals  No Opinion: 1  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 10  Strongly agree: 9 |

## 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.

|  |
| --- |
| * Somewhat Disagree: Digital Twins is not new technology. It’s been around for a while and is relatively mature. (So they have been built with security concerns in mind? CLK) * Not too confident in security concerns designed in technology in the next 15 years. * Yes, but in addition to third parties and maintainers we need to consider the first operator. This is very much overlooked. * No, we are going to be fine because we know about the risk and we will manage it. New technology that will be used in CNI will be recognised as such and will be hardened. There would a problem with technologies designed for other than CNI but which are then used in CNI. * No, there is already response to this kind of problem. UK and US governments banning Chinese technology for example because they do not know what’s in it. * We have to design Technologies for CNI that do not have those vulnerabilities. We should not reduce our standards. * There is a renewed emphasis on security by design. If you are in industry and need replacement sensors or digital twins you’ve got to think about security. Also, there is increase focus on policy, standards and regulation. * We are assuming new technology is not designed with security concerns in mind. |
| Totals  No Opinion: 3  Strongly disagree: 0  Somewhat disagree: 6  Somewhat agree: 5  Strongly agree: 8 |

## 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.

|  |
| --- |
| * My hope is that we're on top of this by 2040. the UK Nuclear regulator is being very proactive about this. They have published a position paper. In the nuclear sector they are doing sandpits to trial AI in robotics, to produce guidelines to develop safety cases. * Yes, the problem is the “unpredictability”. * Do not think we will lose control of AI. The “unpredictability” is about AI not being able to test every possible situation. Generative AI will be introduce massively for certain tasks and with caution for others. It will become more reliable. We will develop all kinds of controls. Will not be perfect, but problems will be easily contained. * It will happen, so I agree with first part. But we need to be resilient to it, we need to prevent it, so I disagree with second part of the statement. AI is being used now for maintenance and to look at vulnerabilities. People may be comfortable with it but it may be ill informing, its very nature hidden from them. * It depends on how well we deal with the problem. * 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. |
| Totals  No Opinion: 4  Strongly disagree: 1  Somewhat disagree: 3  Somewhat agree: 6  Strongly agree: 8 |

## 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.

|  |
| --- |
| * They will try, but might not be successful. AI is not that advanced now. But Yes by 2040. * I hope so. * The CVE index shows a massive rise in AI identifying vulnerabilities in software. People are able to take libraries or pieces of software and train their local language model. * I want to believe that although AI will find vulnerabilities developers will be able to make systems more secure. |
| Totals  No Opinion: 2  Strongly disagree: 0  Somewhat disagree: 1  Somewhat agree: 7  Strongly agree: 12 |

## 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).

|  |
| --- |
| * There are state nations that use misinformation as a matter of course. There are enough people interested the problem, the environment will evolve strategies to deal with it. * It will get worse and do not see it changing in the next 15 years. There are discussions about misinformation and disinformation. People are not going to know what is the truth anymore. * It is already happening. It is a new form of attack which can damage the reputation. * Yes, human panicking can expand to other people. It also depends on the kind of people, who will be the first to panic? who is more vulnerable? Older people, disabled people are less susceptible for example. * It will be an issue and it will be very difficult to do anything about it. The public discourse about CNI failures is enormous damaging. Populations do not trust their governments. So in addition to managing the problems governments need to manage the debates too. * It is possible but at some point there will be a backlash against social media. * People are learning about disinformation, etc. on social media. They are aware of problems and do not take things at face value. * Disinformation is a big issue Now. Wonder if we will get better at responding to it. Question the idea of mass panics. We are a more resilient society. * It is indifference rather than mass panic. People do not pay attention to massive problems. There is not enough moral panic to bring collective action and change behaviours. * Do not agree with “mass panic”. It is not hysteric people running around. It is the use of misinformation to create violent divisions. * Already happening, not sure if it will get worse in 10 years. How does this relate to CNI? * Suggest “general public misinformation.” |
| Totals  No Opinion: 3  Strongly disagree: 0  Somewhat disagree: 4  Somewhat agree: 9  Strongly agree: 6 |

## 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.

|  |
| --- |
| * Poisoning could be potentially undetectable. People would use it without thinking about the risks. * Only a handful of nation states have the ability. One thing is to poison AI to render it inoperative and another thing is to control it, make it do something without the operators knowing it. The latter will be restricted to cutting edge attackers. * It is going to become a bigger problem. * Agree. Would classify this with the other kinds of attacks mentioned. |
| Totals  No Opinion: 2  Strongly disagree: 0  Somewhat disagree: 1  Somewhat agree: 12  Strongly agree: 7 |

## 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).

|  |
| --- |
| * Yes, but I hope we will get smarter on cyberattacks. Not “increase” but “slightly increase”. * Colonial Pipeline - driven by corporate risk? We are not good at managing commercial risks. Commercial dangers as "knee jerk reaction" driven by commercial interests vs Commercial dangers driven by system risks, sometimes as reactions to regulations to keep businesses operating. * Incentives like commercial incentives and profit making are a major problem over security. “Commercial Dangers” means commercial operators not doing security well or seriously? Commercial interests and human interests might be quite different. * Commercial considerations to some extent outweigh resilience. Hope more binding regulation in the US (as dominant software supplier) to make developers/vendors accountable, not only the end consumer. -> Executive order by Biden, shift in the new US cybersecurity strategy. * Absolutely big danger following on from the point about software and hardware supply chain problem. * Did not understand the statement but I think there is an incentive problem. |
| Totals  No Opinion: 5  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 6  Strongly agree: 9 |

## 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.

|  |
| --- |
| * The solutions for the quantum problem are commercial and technical. Doubling the length of the keys won’t work. If quantum works it would be a game changer, especially for CNI because of their legacy systems. * Assume by 2040 the key establishment protocols will be post quantum. "Double the key length" is the current mitigation until we get stronger quantum computers. It will have to come a long way. * 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. * I think it's going to change the world, but not in that time frame, not by 2040. * Pessimistic about quantum. Where is the money? * Confident on this one. Encryption is the perfect application of quantum capacities. It might happen, but it might already have happened. Some country could have developed this technology and keeping it a secret. Some people in the quantum circles believe they might be able to have a hint if it is happening. * Quantum is able to break cryptographic solutions but then intelligence and research is needed to make a proof of concept and make it commercially viable. It is possible but requires an extensive timeframe. Not by 2040. * There is interest about when we will get quantum systems. |
| Totals  No Opinion: 7  Strongly disagree: 2  Somewhat disagree: 5  Somewhat agree: 5  Strongly agree: 3 |

## 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.

|  |
| --- |
| * Electromagnetic storms could happen but not sure if the consequences will be so bad. People are aware of this problem, especially in CNI and build EM hardware resistant. * We’ve been talking about this forever but it has not materialised. Have not heard expert opinion on this. * Haven’t thought about this. Is this fiction? * This has been a concern in the west for some time. It is an issue but with low likelihood. We have never experienced one and we wouldn’t know how to structure these risks. * It will happen but not sure if by 2040. It is going to cause real problems. Scale of the problems depends on what we’ve done to build resilience, and the timing is questionable uncertain. * Been reading this for years, understand the principles and it could a catastrophic event. However, because we have never experienced something like this we do not know what could happen. It is impossible to assess. * It is uncertain, we do not know much. I think we have quite a bit of resilience. (Redundancy communication , Starlink, new types of telecommunication systems). * Clarify what “scale” we refer to. Do not agree with the mass taking of infrastructure. It could lead to short term temporary outages only. * These things can be disrupted by other extreme weather events. Suggest changing “electromagnetic storm” to (extreme, CLK) “weather events”. |
| Totals  No Opinion: 8  Strongly disagree: 0  Somewhat disagree: 5  Somewhat agree: 7  Strongly agree: 2 |

## 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.

|  |
| --- |
| * There are protocols in place for dealing with radio hacks. People might try to get at those but it is hard to see any sort of impact. * There is a trend of talking about more wireless in CNI. In nuclear they are much slower to adopt wireless and radio for control and monitoring systems, but in other sectors it might be quicker. In 20 years I haven’t seen cyberattack using radio interception. Maybe people do not report it. * Not sure about nuclear, but in 15 years wireless would have replaced wires. * Not worried about radio hacks. Does not seem a key risk. There is lots of good work around radio. * Unlikely to happen If they use radio there will be strong encryption like in wi-fi. * Why would they use radio communications in nuclear stations? Maybe if risks and impact are low, otherwise don’t use it. * Don’t see this happening. Satellite hacks are more of a concern than radio hacks. Young people don’t know how to operate a radio properly, in the west. * Everyone know radios are a bit susceptible. But we have a range of technologies: some radio based, some digital switch packed based systems, fibre, copper. We don’t rely only on one technology. * Agree with the use of wireless increases vulnerabilities. Disagree with successful cyberattacks using radio interception. Systems should be designed to reduce vulnerabilities and chances of cyberattacks. * Don’t know much. Never heard of this before. Are they putting radio technology in nuclear plants? * Radio hacks are a not so obvious risk. People are not paying attention to it. |
| Totals  No Opinion: 4  Strongly disagree: 3  Somewhat disagree: 6  Somewhat agree: 9  Strongly agree: 0 |

# MITIGATIONS

**Description:** General Comments about Risk Mitigation Strategies, Parent code

|  |
| --- |
| * Adaptation rather than Mitigation. Suggest grouping mitigations e.g. mitigations about people using technology. Mitigations are linked, we could group them following those connections. * Prioritise and focus on priority outcomes or activities first. * We have to look at the mitigations as a combination/collective rather than individually. They complement each other. Not one control or a group of controls will give you complete defence in depth and protection. |

## 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.

|  |
| --- |
| * Resilience has to be a key property of a system . Resilience is connected to sociotechnical. * Resilience approaches are not new. In the 2000’s no one paid much attention. But now a lot of people are looking at resilience and sociotechnical. * Suggested resilience practices: systems thinking, systems engineering, adversarial red teaming and from the design point of view: decoupling error detection and correction, graceful failure and duplication. There are complexities that create fragile conditions, there are complexities that create anti-fragile conditions, we should seek the second. * Resilience has two aspects: resistance to perturbation and restitution to status quo/new acceptable state. It is difficult to distinguish between kinds of attacks. Resilience has to account for both, for perturbation and restitution. We should start from Resilience, not from incident prediction, etc. * Personal opinion: systems diversity is the means to systems resilience. Antitrust action, trust busting data can help Systems. Resilience * 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. * We need to define Resilience, Systems Resilience and Systems Approach (we do not mention systems approach or systems thinking in the report, CLK). Suggest a systems thinking/holistic perspective of problems. And actor network theory to talk about systems of systems. * With resilience, we can respond and recover. We can deflect attacks and those attacks won’t be that severe, we could tolerate them more. * We need all kinds of controls not only resilience. * There's a whole big literature on resilience. I'm not a massive fan of the concept, but it's important. * Systems resilience and secure systems by design should be built into the cloud. The scope for individual infrastructure organisations is in a way quite small. * The key thing is that it's a systems problem. |
| Totals  No Opinion: 1  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 2  Strongly agree: 16 |

## 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.

|  |
| --- |
| * Free open source vs Commercial. For open source it is not clear whether the OS community provides high security. It could be a security risk. If the community is large and active, and have low, medium and high security standards I could assume high OS is usable. With commercial you can take OS and add engineering work, design work, check, test and verify the code. You need more expertise for that. It is no longer writing code only. It becomes a product. * Secure by design focuses on products, individual components, not on the overall system. A secure component cannot be used anywhere this is why whole system design is more important than component system design. * We need systems to be secure by design but do not agree with Cheri Morello and RISC-V architecture. * Secure by design is better than no secure by design but it will not solve all the problems. * Secure systems by design is about making sure there are enough layers of defence. The more layers the higher the cost. There could also be human layers. Aim is an affordable mitigation. We have to look a the overall problem and see what applies best. It could be education of people or policy. * Secure by design has a direct impact on resilience. * Secure by design is important but don’t know if it will happen. * US approach: to make secured by design binding. UK: lots of efforts, more voluntary than legally binding. Secure by design impactful way to mitigate. * Most people’s environment nowadays is the cloud. Systems resilience and secure systems by design happens in the clouds. (Most if which not design in the UK.) The negotiation has to be with the suppliers. * Thinks resilience is the aim but when talking to computer scientists they think secure systems by design is the key, that it is possible to write secure code up to the microkernel level. |
| Totals  No Opinion: 1  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 3  Strongly agree: 15 |

## 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.

|  |
| --- |
| * Did some work on quantitative risk management. It was pretty good. We can measure risk to the nth degree and use fancy models but not sure how to make it cost effective. * Risk features heavily on governments secure by design principles. Risks is a vehicle to talk about resilience. Risk management should be employed more widely and from a design perspective. * People should be doing it now. We are not good at it. * Companies cannot work like the secret service. Companies use excel files to write and assess potential risks. Do not thing it works, but at least companies can claim they are doing it. Companies focus on the high probability risks, looking at everything won't support the daily way of working. It could become overwhelming or complex and expensive. When the system is complex, risks, consequences, counter measures have to be visible to the system architecture, to the designer to the management level. It has to be a risk management process included in the system design. There is a difference between everyday work/risk and risks which are unusual not part of the business process. * Risk management is costly, time consuming and very unreliable/we can’t predict everything. * Risk management needs to happen. It will be a lot of work. Civil services are risk ignorant and take risks no commercial organisation would take because they do their numbers. There are certain areas of proper engineering where you get to do risk management, but commercial risk management is “sacrificing chickens”. * Risk management is pretty mature in the financial sector. But it isn’t mature everywhere else. * 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. * Risk management is quite poor in CNI. Education is needed. * Is investment in risk management: putting things in place or management systems for risk? We can do all risk assessments but it will only work if we implement it in practice. * Risk management includes the human factor. * Tracking attacks and failures allows to do risk management. Tracking gives us the numbers for risk management which allows resilience. |
| Totals  No Opinion: 2  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 6  Strongly agree: 11 |

## Question: Training of professionals

**Description**: Integrating security and resilience into software education; improved training about software contracts.

|  |
| --- |
| * Lots of problems will go away if there was proper training. In CNI there are different areas of knowledge. There is knowledge asymmetry. This is a big problem. Education will help with awareness. * Agree with statement but it is not enough. We need to design good from scratch from the beginning. * “Education of Stakeholders” and “Training of professionals” are two parts of the same thing. Certain professionals will be stakeholders in other people’s stuff. Wording: some people are “trained” whereas others are “educated”. Does it mean that we push stuff onto them so they understand and know what to do? * Training does not reduce the risk. It is only when people who are trained do something about it. |
| Totals  No Opinion: 2  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 3  Strongly agree: 15 |

## Question: Systems testing including red teaming

**Description**: Testing and verification for entire systems, including human operators.

|  |
| --- |
| * Red teaming is an important resilience approach. * Feel like verification has not helped that much yet. It is taking too long for it to work. * Red teaming is a specific military term. Try using a more generic term like testing and exercising. Include ethical hacking. This is about checking how systems work and finding weak points in security. * UK is falling behind. There are no resources. More work needs to be done. * Testing and red teaming are successful ways to prepare for ransomware attacks. * It’s definitely is going to be important. |
| Totals  No Opinion: 1  Strongly disagree: 0  Somewhat disagree: 1  Somewhat agree: 5  Strongly agree: 14 |

## Question: Research into Sociotechnical approaches

**Description**: Research into the non-technological/human aspects of CNI system security.

|  |
| --- |
| * Sociotechnical is linked to resilience and can expand into managerial, cultural and organisational issues. * 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. * Research needs to be done, and needs to be better communicated. Problem is lack of investment, lack of interest from seniors, and the fact that this space is dominated by techies. * Research is important but I would prefer to build systems which include sociotechnical bits, which are easier to use the right way and harder to use the wrong way. Design a system that involves the human. * “Research into sociotechnical approaches” is too vague. Also, “… aspects of CNI system security” is too specific. It is more that system security. It is many aspects like software design, security, user interfaces. It is those technologies in the CNI sites. * Sceptical about this type research because of psychological bias and replication problems. |
| Totals  No Opinion: 1  Strongly disagree: 0  Somewhat disagree: 1  Somewhat agree: 4  Strongly agree: 15 |

## Question: Legislation and government support for resilience

**Description**: To address the ‘commercial dangers’ problems.

|  |
| --- |
| * Legislation is important but taxpayer can't do everything. Tax to help businesses be more resilient? Is it not the business's job to do that? The market runs the economy not the government. * What are the “commercial dangers” and what specific support do we need? * We are still regulating for security not resilience. The UK is 5 to 10 years ahead in legislation for resilience. It is regulation rather than legislation. E.g. anti fraud strategies - financial institutions are held responsible. Their regional resilience centres are enabled by legislation but it is really Regulation. * 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. Legislation for resilience is super important. Training and education are important but not the solution to the lack of support at the top. * Powerful tech companies are not likely to agree to government led templates for contracts. Software suppliers have standard contracts (terrible or not) and procurement organisations do not have the power to modify that. * There are incentive problems. Fixing the incentives will fix a lot. |
| Totals  No Opinion: 1  Strongly disagree: 1  Somewhat disagree: 2  Somewhat agree: 1  Strongly agree: 16 |

## Question: Education of stakeholders

**Description**: Training about the dangers of AI-enhanced ‘phishing’, and more basically, about what digitalisation means for their roles.

|  |
| --- |
| * In CNI there are different areas of knowledge. There is knowledge asymmetry. This is a big problem. Education will help with awareness. * We need to educate people on AI. * Education is important but it is not enough. We need to design good from scratch. * If education was going to help, it would have happened already. Education is important, but focus should be on design. E.g. why is phishing possible? Because of broken authentication mechanisms. A lot of what education tries to do should be done by secure by design. * Training of professionals and education of stakeholders are the same point. Do we use the word stakeholder for “other people” we want to understand things? * Biggest issue is not the technical individuals but, senior stakeholders/management, the procurement, directors, engineer managers. They have not been educated in the dangers, etc. Education should be number1 but this should be a combination of efforts, e.g. systems resilience approach is multimodal. * Training does not reduce the risk. It is only when people who are trained do something about it. * I'm not sure we can educate our way out of this problem. We can educate, run public awareness campaigns, etc. but there will be lots of exploitable vulnerabilities. * Training and education go hand in hand but education is more important. (Tech) professionals already have baseline understanding, but stakeholders do not. Educating stakeholders would eliminate human weakness. |
| Totals  No Opinion: 2  Strongly disagree: 0  Somewhat disagree: 1  Somewhat agree: 6  Strongly agree: 12 |

## 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.

|  |
| --- |
| * There are some interesting military projects using Machine Learning for Offensive Hacking. Digital Twins can be used to model and understand systems… “how to understand an injection into intervention” (? CLK). |
| Totals  No Opinion: 3  Strongly disagree: 0  Somewhat disagree: 1  Somewhat agree: 9  Strongly agree: 8 |

## 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.

|  |
| --- |
| * I think it’s probably coming. * Training can only do so much people forget what they learn the day before. Situation awareness does not work like this (CLK?) Need to change the design of the system. Wording AI/New Technology can help... * AI would be only part of the solution. * AI will have a role but will not solve all our problems. AI can add another layer of complexity and obfuscation because we cannot understand what the algorithms do. It is dangerous to think technology will solve our problems. We have to be careful with the kind of technology layers we add to our existing systems. * There are benefits from using AI for incident management in different areas. Generative AI can be used for playbook development, testing data or support people to code. A lot of incident management is workflow based which works well with Generative AI. We need to communicate what could be done with AI. * AI is going to be part of the solution. * Technology for incident management, I think, makes a lot of sense. Technology can identify anomalous situations based on existing data. It can help us understand and not ignore part of the picture. |
| Totals  No Opinion: 4  Strongly disagree: 0  Somewhat disagree: 1  Somewhat agree: 12  Strongly agree: 4 |

## Question: Systems diversity

**Description**: Regulation and guidance to promote software (and hardware) diversity, to create resilience against vulnerabilities.

|  |
| --- |
| * Commercially unattractive with limited benefits. * Diversity (as a resilience mechanism) is hard to achieve and verify. * Agree. This is what we teach. * It is being done but they ignore the human side of it. * Diversity of component and different failure mechanisms are part of systems resilience. * Do not agree with “regulation,” Designers need to conclude they need diversity rather than being told to do it by regulation. * Systems diversity as part of systems resilience. * Systems diversity means having multiple systems running in parallel which is massively costly. This could be achieved by governments but not in the commercial sector. * Is systems diversity not part of systems resilience? If the point of this mitigation is about regulation then the description is not good enough. * Important. Two things can’t fail at the same time. * Not sure if diversity creates resilience. Some research states we need to go the other way around, going for less suppliers, less systems so we know what happens to them. (Less diversity - less complexity CLK.) * Two counter arguments. Intuitively: systems diversity creates systems resilience. But, not everyone has their own fiddly, improvised solutions. It is not easy to secure dozens of systems. - Non-diversity can work as long as we hold large vendors accountable. * Not sure how much diversity can be achieved when these networked environments always end up with the same 2 or 3 competitors. |
| Totals  No Opinion: 3  Strongly disagree: 0  Somewhat disagree: 5  Somewhat agree: 4  Strongly agree: 9 |

## 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.

|  |
| --- |
| * Not sure if legislation is the key. It is a security maturity question. If you are immature you do not know what to do with that sort of data. If you are mature, you are probably already doing it. There are (mature) networks in Europe and probably UK where information sharing already exists. * Legislation always messes things up. Do not know if data can be anonymised. Who to trust to keep that sort of data and not be breached? * There is a tension between sharing data on attacks and failures and sharing data without exposing existing infrastructures further. * We need radical transparency in these systems, but we can’t do it in isolation. There is already a "cybersecurity information exchange" model that works behind the scene successfully. Banks meet with NCSC to discuss their security problems. Banks do not use this information for commercial reasons. They know they are doing this for the whole sector. They have tried to setup similar mechanisms for other industries but it takes time to get trust. - Tracking attacks, etc. should be given a serious thought but it should but be rushed into panic. * We already have the NCSC reports. “Legislation” about sharing of anonymised data is not in scope. * We cannot force people to share things. Organisations do not trust each other. People do. We would need a trusted organisation which is cybersecure and human secure,.... it would be impossible. Issue of sharing information with organisations in countries sympathetic to our opponents. * It would be appropriate. * The current/outdated Computer Misuse Act 1990 criminalises what security teams need to do in order to understand threats. Professor Audrey Guinchard, from University of Essex, wrote a paper about this and is involved on reforming the act with the Criminal Law Reform Now Network. (This might be the paper: Guinchard, A. (2018). Taking proportionality seriously: The use of contextual integrity for a more informed and transparent analysis in EU data protection law. European Law Journal, 24(6), 434-457. - Also: Reforming the Computer Misuse Act 1990. Criminal Law Reform Now Network Report. 2020 http://www.clrnn.co.uk/media/1018/clrnn-cma-report.pdf CLK) * We really need Tracking attacks and failures. It is very important that is made widely available as possible. The government does not provide this kind of services. There are private companies who step into government shoes to sell this intelligence because companies need this knowledge. * It might be a legislature overreach and there might be some pushback against it. More sharing is good but not sure it can be legislated on that scale. * Tracking existing attacks and failures should be number one in the list. It is crucial for IT suppliers, etc. to know this information. Suggest using the NIS Framework to track real events, damage to Jas (? CLK), health and life, financial damage for maintenance. Also, continuous monitoring of small incidents on CNI is very important, as they are complex and tighly couple systems. This data would be useful to build up data to anticipate and prevent major failures. Check "natural accident theory". Check Ed Steinmeller paper on measuring user impact of failure. (Could not find the paper. CLK) * From a deterrence theory approach, expanded shield, shared defence view, this is still not solved. |
| Totals  No Opinion: 1  Strongly disagree: 0  Somewhat disagree: 2  Somewhat agree: 10  Strongly agree: 8 |

## Question: Diplomacy around cyber threats

**Description**: Threat of military response to serious cyberattacks; imprisonment of hackers captured while travelling.

|  |
| --- |
| * Not convinced it will be effective. People will not reveal the capacity they’ve got. * We need to talk about this, threat of military response to cyberattacks. * It is important. I’ve been involved in diplomacy around cyberthreats and sharing cybersecurity information. - Hard part is diplomacy creates sides/blocks/coalitions against the other. * Not convinced despite the risks. * We need a channel of dialogue, to agree what is acceptable and not. * Don’t think it will work. * Understand that is something that needs to happen. Need to be clearer with statement: what political and diplomatic activity is needed to defend against cyberthreats? * Diplomacy is key. People are aware of cyber but they are not necessarily aware of how cyberthreats apply to their individual use cases. * Diplomacy is important but it will not solve all problems. There have been very few circumstances where there has been a military response to cyberattacks, the US killing an ISIS hacker, imprisonment of hackers when they travel. There are ethical and law barriers. Response has to be proportional. More common diplomacy around sanctions which are important to shape international behaviour. Also, treaties and police cooperation. |
| Totals  No Opinion: 6  Strongly disagree: 0  Somewhat disagree: 5  Somewhat agree: 6  Strongly agree: 4 |

## Question: Research into sociotechnical errors

Description: Academic research into why human errors happen, and ways to mitigate social engineering.

|  |
| --- |
| * This kind of research has been happening for a while. E.g. Sasha Brostoff PhD on human error in security from 2000. However there has not been any impact so far, e.g. around mitigating social engineering. * Yes, we need to dive deep and ways to mitigate social engineering. There is support for it from psychology and behavioural science. * It is important. We need to pay attention to it and design it into our systems. It doesn’t happen now because of budget and time constrains. * Agree. It is a sociotechnical problem because of seniors and lack of investment. Because the sector is dominated by the techies. When budgets are cut, sociotechnical is the first thing to go. * Consider adding ‘Social Engineering in the context of information security’. Also consider all research done on human errors in high risk critical industries which can be applied on cyber risks and CNI. * Agree, it is about understanding why human errors occur. * These kinds of errors will continue. * Research into sociotechnical errors is included into research into sociotechnical approaches. What would make a change is the training of professionals and education of stakeholders using Research into sociotechnical errors as input. |
| Totals  No Opinion: 1  Strongly disagree: 0  Somewhat disagree: 1  Somewhat agree: 8  Strongly agree: 11 |

## Question: Business as Usual Cybersecurity Research and Practice

**Description**: Activities that are currently being strongly promoted and carried out.

|  |
| --- |
| * If we continue business we might not address important things that need attention. * As I agree with the other mitigations I don’t support doing business as usual. * Business as usual will not work. It means mono disciplinary efforts and fails to understand cybersecurity and cyber resilience as a system. What is needed is to bring different kinds of expertise. I think the government (Canada? CLK) are trying to develop new funding models/streams which consider these systemic approaches. * We need to step up the status quo approach. We need more resources and budget to do more. Problems can get worse if we keep doing the same amount. * Does this mean lets keep doing what we are doing if it is good? |
| Totals  No Opinion: 5  Strongly disagree: 1  Somewhat disagree: 5  Somewhat agree: 5  Strongly agree: 5 |