

Software Risks for Critical Infrastructure towards 2040: Dataset: Highlighted Comments and Revised Statements

|  |  |  |
| --- | --- | --- |
| **C. Loureiro-Koechlin** Lancaster University | **L. Dennis** University of Manchester | **C. A. F. A. Weir** Lancaster University |

Copyright © 2024 Lancaster University, University of Manchester

**2 September 2024**

# Introduction

This document was created by the researchers as part of the Delphi Study. It contains the anonymised participant comments on each statement from the Round 1 report, along with the rewritten statements for the next version of the report.

# What is CNI?

1. **Definition of CNI**: Definitions of CNI have varied considerably, from ‘sufficient infrastructure to recover from nuclear attack’ in the UK in the 1950s, to ‘anything politically sensitive’ as appears to be current in the USA; definitions vary as technology changes. The current official UK definition is of services in thirteen sectors where incidents could lead to major loss of life, casualties, economic or social impacts; or impact national security or state functioning[[1]](#footnote-2). Much of CNI is in the private sector, and services making up the supply chain to CNI are therefore themselves critical.

|  |
| --- |
| * 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. |

1. **Longevity of software**: much CNI software and infrastructure is long lived: up to many decades. It is hard to preserve developer knowledge over those timeframes; that and safety concerns can hinder modernisation and the removal of vulnerabilities.

|  |
| --- |
| * 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. |

1. **Commercial drivers**: CNI are operated by public and private sector organizations; commercial visions may impact technology strategies and their implementation. However, innovation is mainly led by government discourse, often through spin out companies of people that understand CNI.

|  |
| --- |
| * Industry isn’t that influential - it is hard to share tacit knowledge about CNI. * Legacy systems demonstrate little to 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 |

1. **Use regulation to coordinate CNI response to risk**: Organisations in highly regulated sectors, such as nuclear, energy and health, work together with government to provide regulatory bodies, forming an industry consensus on defining their response to risks.

|  |
| --- |
| * 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. |

# Expert Forecasts - Trends

The experts identified a range of trends affecting the potential for major incidents related to software, as follows.

1. **IoT and other next generation technologies**: 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. Rates of adoption will vary by sector; for example, transport is already adopting all of these technologies, whereas utilities and nuclear will take much longer.

|  |
| --- |
| * 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. |

1. **System complexity and interconnectivity**: by 2040, CNI systems will have increased software complexity and interconnectivity, though less so in highly regulated sectors. This will make it more difficult to understand the complex sociotechnical interactions involved and will in some cases make systems more vulnerable to human error and to attacks.

|  |
| --- |
| * 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. |

1. **Increase in digitisation**: Towards 2040, most infrastructure will become software-controlled, to simplify control, increase efficiencies, decrease costs, and provide data accessibility.

|  |
| --- |
| * 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. |

1. **Decentralisation of services**: 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, perhaps including nuclear in the form of Small Nuclear Reactors. Centralised control will still be the default in most cases.

|  |
| --- |
| * 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? |

1. **System operators working through software, not directly**: By 2040 humans’ participation in CNI processes will increasingly be through complex software systems rather than directly with hardware or simple software controls; however, analogue systems and direct human participation will still remain, especially in safety-critical systems.

|  |
| --- |
| * 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 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.- DONE * 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. |

1. **Increased end-user dependency on technology**: 2040 will continue to see increased reliance by consumers on software, data and machines to plan and carry out activities. In CNI, humans will be kept in the loop for critical functions.
2. **Changing geopolitical context:** may impact the Internet and the information it holds by segregating it into separate blocs with differing values and standards, though telecommunications standards will remain global.

|  |
| --- |
| * 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 too 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.  NO, 3 WASN’T. MOVED TWO HUMAN ONES TOGETHER.. * We depend on technology, on data. Data is used as a point of reflection to see where we are and what we are doing. |
| * Busy question. There are different parts to it. |
| * Somewhat disagree. Geopolitics has an impact now. There will always be state/nation interests. There will not be any substantive change. * Not sure about the first statement. * 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. * 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. * Agree with separation of internet. * Agree with both. Solar panels have been driven by climate change. * The world has been divided into blocks for centuries. Do not think there will be a separation of the internet: having private spaces for CNI - General Internet. * Internet segregation has been predicted for 20 years but still has not happened. |

1. **Climate change:**  will continue to drive digitisation and automation to provide solutions to mitigate harms, such as distributed systems to support greener energy.

|  |
| --- |
| * What does “CNI to implement changes to mitigate harm” mean? What are the changes? Distributed energy generation is already happening. * In terms of climate change we are already doing it. We are providing requirements, planning for the future. * In terms of climate, CNI is already doing that. People working in CNI want to make those changes. * Do not understand the second part of the statement. * Not convinced with climate statement. * 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. |

1. **New CNI**: Aspects of the internet (‘the cloud’) have already become critical infrastructure, even if they are not defined as such; this trend will continue with increasing digitisation towards 2040.

|  |
| --- |
| * 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. |

1. **Artificial intelligence**: Towards 2040, advances in Artificial Intelligence (AI) will open doors to increased and improved automation, better situational awareness, and better data interpretation; as well as the development of safer, more efficient, and more effective systems. However, it will also bring increased risks, such as deep fakes and unpredictability.

|  |
| --- |
| * 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. |

1. **Quantum computing**: will not have a major impact by 2040; it will be only for a few international companies and nation states and will be supported by AI techniques. Quantum breaking of cryptographic encryption might be possible then, though easily mitigated by algorithm changes. Quantum techniques for secure communication will be used in some cases.

|  |
| --- |
| * 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 75y 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. |

1. **Off-the-shelf hardware and software**: Towards 2040, some CNI systems will increasingly be made from off-the-shelf hardware and software components. However, this will bring risks where they are not built to a high enough standard. Many CNI operators will still prefer to develop bespoke systems or to strengthen their off-the-shelf 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. |

# Expert Forecasts - Risks of Major Incidents

This section explores the factors that might lead to a major incident. Software-related risks vary enormously in probability and likely impact; and may relate to malicious actors, human error or both. There will also be ‘unknown’ risks, yet to be identified.

1. **Poor response to accidents or attacks:** The response to adverse events is key part of what makes them ‘major’ or otherwise. Though much of CNI is run by well-prepared mature large companies, towards 2040 we shall see increasing difficulty in identifying and responding due to:

|  |
| --- |
| * Poor response will still happen but it won’t increase exponentially. * Poor response means people do not do what they are supposed to do. * 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. * Failures occur when systems are not designed properly. * There is 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. |

1. Poor human response due to lack of government-led preparation, lack of training, lack of sharing of key information, trust in bad quality data and poor human factor aspects of systems;

|  |
| --- |
| * Not enough people with the right skills. There is no direction towards development of new capabilities. * 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. * 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. * 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. * No knowledge or intel is shared. Human factor is key. |

1. New forms of malicious activity as actors become more sophisticated; or

|  |
| --- |
| * Is it additional or different malicious activity? Worries about state aligned threat actors. * 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. * The problem is when attacks are so sophisticated that there is no response planned/possible. |

1. Issues with AI-based situational awareness and guidance.

|  |
| --- |
| * We will probably get better at automation. * The more AI gets into society the more glitches we’ll see. * Agree with B. and C. * People are being careful about AI at the moment. |

1. **Attacks via Humans**: Towards 2040, most cyberattacks will continue to involve humans and machines: both insider threats and external 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. Improvements in social engineering techniques and deep fake technology will exacerbate this problem.

|  |
| --- |
| * 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. |

1. **Cascading Problems**: Towards 2040, increased interconnectivity, due to extensive use of IoT, 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 in advance.

|  |
| --- |
| * 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 design 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. |

1. **Software and hardware supply chain problems**: 2040 will continue to see increasing issues with the provision of software components, software services, hardware supplies, system maintenance and related services. This will be exacerbated by the international nature of such supply chains, despite work being done to map and understand them. Further obstacles will include the disconnect between technology users and developers, the disconnect 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 if 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. |

1. **Sociotechnical problems**: By 2040, digitisation, increased complexity and poor human factors in design of systems (a term that includes the operators and users), will lead to increasing disruptions even when all the participants are working in good faith[[2]](#footnote-3).

|  |
| --- |
| * 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. They are the more common form 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 in interconnectivity is the source of the risk. * Not sure if digitisation is the problem. |

1. **Breakdown of electricity, telecommunications or internet**: By 2040, much of CNI will not be able to function without these. Electricity in particular is easy to disrupt, and failure may cause cascading problems. 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 failure is an example of a cascading problem. |

1. **OT attacks**: Operational Technology (OT) used to be relatively safe because of the obscurity of its programming and the isolation of OT systems. However, towards 2040, OT will increasingly be integrated with Information Technology and IoT technology, making it easier for cyber attackers, especially nation states, to connect and disrupt 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. |

1. **AI-based phishing, whaling and similar attacks**: 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. |

1. **Common mode failures**: Towards 2040, widely dispersed systems will increasingly have monoculture technologies (systems, components and vendors) for portions of their operations, which will thus share the same vulnerabilities. These will allow mass replicated attacks or lead to cascading problems.

|  |
| --- |
| * 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. |

# Risk Mitigation Strategies

Our experts suggested a range of complementary approaches to address the future risks they identified. Such ‘mitigation approaches’ address and reduce the wider problem in addition to improving defences and the response to incidents.

1. **Systems Resilience approach**: Designing and organising to provide *resilience* in addition to cybersecurity: the capacity to endure and adapt to disruptions. Resilience is a feature of an entire system (of systems); addressing it might involve incident planning, red teaming, redundancy in provision, design for gradual degradation and enforcement of systems diversity. Resilience research can include systems thinking and actor network theory.

|  |
| --- |
| * 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. |

1. **Secure systems by design (SSBD)**: Incorporating systems security, privacy and safety analysis—including human interaction analysis—from the earliest stages of design in creating and modifying software systems. By focusing on individual products and components, SSBD delivers layers of security and provides a path for upgrades.

|  |
| --- |
| * 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 secure 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. |

1. **Improved risk management**: Supporting organisations to systematically identify, understand, and assess potential threats, integrating these practices into both system design and ongoing processes, to support focusing on risks with a high expectation of loss rather than just high probability. While well-established in finance and healthcare, risk management needs broader adoption in other industries to enhance cybersecurity resilience, with an appropriate light touch to avoid it becoming costly and unwieldy.

|  |
| --- |
| * 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 in 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 think 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. |

1. **Training of professionals:** ensuring consistent education of software and domain expert professionals in both theoretical and practical aspects of security and resilience across all levels, including the implications for software contracts to define responsibilities and liabilities around cyber risks

|  |
| --- |
| * 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. |

1. **Research into Sociotechnical approaches**: Research and research dissemination covering the human, non-technological, aspects of CNI system security, software design and user interfaces. Though this research is difficult for traditional cybersecurity researchers, and subject to bias and replication problems.

|  |
| --- |
| * 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 than system security. It is many aspects like software design, security, user interfaces. It is those technologies in the CNI sites. * Sceptical about this type of research because of psychological bias and replication problems. |

1. **Adversarial systems testing including red teaming**: Promoting adversarial testing for entire systems including their human users and support staff. Techniques include both ethical hacking, and social engineering approaches.

|  |
| --- |
| * 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. |

1. **Legislation, regulation and government support for resilience:** to motivate organisations to invest in systems resilience, secure by design approaches and adversarial systems testing.

|  |
| --- |
| * 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 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. |

1. **Education of end users:** Training for end users at all levels about the dangers of AI-enhanced ‘phishing’ and about what digitalisation means for their roles. While no substitute for appropriate human factors and system design, this can reduce the immediate risk.

|  |
| --- |
| * 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. |

1. https://www.npsa.gov.uk/critical-national-infrastructure-0 [↑](#footnote-ref-2)
2. As happened in the Three Mile Island and Chernobyl incidents. [↑](#footnote-ref-3)