The Human Factor: Addressing Computing Risks for Critical National Infrastructure towards 2040

7 April 2025

Charles Weir[a]
charles.weir@lancaster.ac.uk

Cecilia Loureiro-Koechlin[a]
cecilia.loureiro@gmail.com

Lucy Hunt[a]
l.hunt1@lancaster.ac.uk

Louise Dennis[b]
louise.dennis@manchester.ac.uk

[a] Infolab21, Lancaster University
Lancaster LA1 4WA, UK

[b] Kilburn Building, University of Manchester
Manchester, M13 9PL, UK

Abstract

The authors conducted a UK-based future study employing the Delphi method to explore the impact of emerging computing technologies on Critical National Infrastructure (CNI). The study engaged 22 domain experts specializing in software, cybersecurity, and CNI, whose roles all include forecasting technological trends and challenges. The findings propose making Internet Services a CNI sector, and suggested the weightiest concern to be human-centric challenges around the recovery from software disasters and cyberattacks. Other major concerns also related to human factors, such as attacks via operators, and errors stemming from poorly designed human-computer interfaces. The suggested mitigation strategies therefore concentrate on human-centred approaches. Key recommendations include promoting human-focused cyber resilience, and using legislation, regulation and standards to help establish it in CNI organizations.

Keywords

Cybersecurity, Critical National Infrastructure, CNI, Delphi method, Cyber resilience, Future studies.

1. Introduction

The rapid advancement of modern technology introduces a series of risks which could potentially impact Critical National Infrastructure (CNI) systems, as well the society and individuals they serve (UK Government, 2023). As technologies evolve, they often outrun existing security measures, making CNI systems vulnerable to attacks, accidents and failures (Raban & Hauptman, 2018). The interconnectivity of the systems and the increasing reliance on

digital technologies intensify these risks. Therefore, having a comprehensive understanding of the systems and their potential risks is imperative to ensure the continued operation of CNI services.

1.1. Background: What is Critical National Infrastructure?

Definitions of 'Critical National Infrastructure' vary considerably, from 'sufficient infrastructure to recover from a nuclear attack' in the UK in the 1950s (UK Government, 1948), to 'anything necessary to our way of life' as current in the USA (CISA, 2024); definitions also vary as technology changes. The current official definition from the UK National Protective Security Authority (NPSA) defines Critical National Infrastructure to involve thirteen national infrastructure sectors as follows:

Chemicals	Civil nuclear	Communications	Defence	Emergency services
Energy	Finance	Food	Government	Health
Space	Transport	Water		

Not everything in each sector is seen as critical, of course. CNI is (NPSA, n.d.) "*Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:*

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

2. *Significant impact on national security, national defence, or the functioning of the state".*

So, for example, the WannaCry ransomware attack on the NHS was considered a CNI incident; a cyberattack on a school would not be.

The full scope of CNI is therefore very wide.

1.2. The Problem: Changing Software Situation Related to CNI

Along with most organisations of the 21st century, CNI suppliers rely heavily on technological systems, including hardware and software to automate processes, provide monitoring, support data analysis and facilitate decision-making.

The vital role of CNI in ensuring the smooth function of society and maintaining public safety, combined with their unique operational conditions, makes the identification of risks threatening their functionality crucial. Safeguarding CNI systems is essential to prevent disruptions that could have widespread and severe consequences.

This research explores future problems associated with the software systems used to operate CNI. As researchers, we started with the presumption that the current state of cybersecurity in CNI is acceptable. This seems reasonable, given that cybersecurity issues have a low priority in the UK National Risk Register (UK Government, 2023). We therefore wanted to know whether changes affecting software systems, especially changes in technology, could lead to a situation where the impact of cybersecurity problems becomes unacceptable. As researchers and engineers we also wanted to discover how research and other changes might prevent this from happening.

This study therefore explored the following research questions:

> *RQ1: What effect may change in the nature and use of software systems between now and 2040 have on the potential for major incidents related to UK Critical National Infrastructure (CNI), especially as related to the Civil Nuclear, Communications, Energy and Health sectors?*
>
> *RQ2: What actions can we as a society take now to address the resulting risks?*

1.3. Technology Forecasting Methods

Future studies are now a well-established discipline, with its own conferences and experts (Slaughter, 1998). Technology forecasting is a major component of this.

It is, of course, rarely possible to predict the future reliably. The science of looking forward to the future relies therefore on forecasting: characterizing each of several outcomes, with some idea of the likelihood of each outcome and of what events and developments might lead to each coming about. The academic methods for predicting technological change include macrohistory, Field Anomaly Relaxation (FAR) and Delphi studies.

Macrohistory is the sociologically informed analysis of long-term patterns of political, economic, and social change (Collins, 1999). Macrohistory researchers identify trends in past history as a basis for extrapolation into the future. It enables a rigorous approach to analysing social trends; however, it is not commonly used as a basis for technological prediction. Macrohistory is often used as a source of data when combined with other methods of analysis.

In FAR, researchers identify a set of different topic areas, called 'sectors' (Coyle, 1997). They then use interviews with experts, literature surveys, and a range of other techniques to identify many different outcomes ('factors') over time in each of the sectors. They then use 'relaxation', identifying incompatible combinations of factors, to focus in on a small number of total outcomes ('scenarios'), which are often expressed as timelines. FAR can be remarkably effective, but is heavyweight and time consuming (Rhyne, 1981).

The Delphi method involves several rounds of interviews with experts until a consensus has been reached. This is labour-intensive, requiring multiple experts to spend time speaking with researchers, to provide some measure of what experts think. Delphi studies are widely used in situations where there is expertise, but little concrete information. Such situations include policy and strategy creation in a wide range of settings, including forecasting. The Delphi method has two advantages over more direct methods of gathering expert opinion. It is anonymous, which encourages participants to be honest and open in their feedback. And it is iterative, allowing for feedback between participants so the results are refined with each iteration (Beiderbeck et al., 2021a).

The remainder of this paper is as follows. Section 2 describes the study's methodology; Section 3 explores the study results, including participant descriptions; Section 4 discusses the results, comparing them with prior work, discussing limitations, and exploring two recommendations in more detail; and Section 5 provides a conclusion with strategy recommendations.

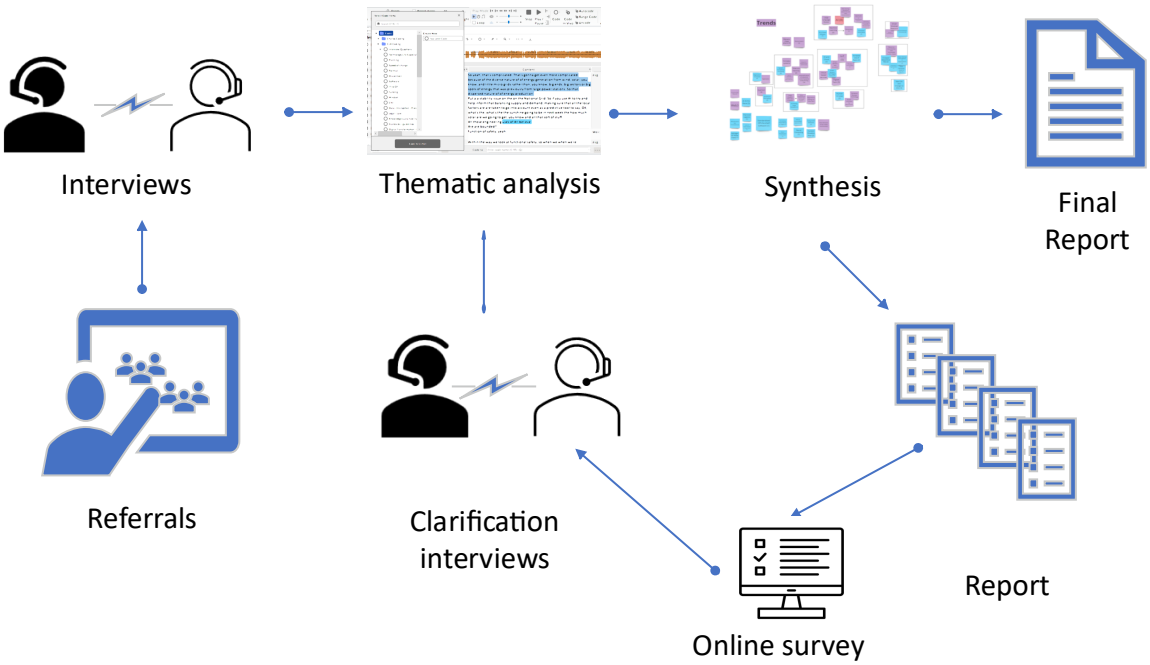

Figure 1: The Two Round Delphi Study (excluding literature review and workshop)

2. Study Methodology

While the primary research question RQ1 covers forecasts about the changes in technology, RQ2 asks for further, non-forecasting, insights. We therefore chose a Delphi study over FAR or macrohistory, since this approach can handle a wider range of topics. Specifically, we carried out a two-round interview-based Delphi study, followed by an in-person workshop.

This method enabled the identification of emerging technological trends, the identification of contextual factors, including technological, economic, social and human, while capturing a range of diverse perspectives from experts. The study involved an initial literature survey, followed by semi-structured interviews and surveys with experts in CNI security, policy and technical specialities. In line with the Delphi study methodology we did not incorporate other findings and sources into the survey itself (Beiderbeck et al., 2021b). Our Delphi study approach is shown in Figure 1 and described in the following sections.

2.1. Recruitment

We recruited professionals whose roles involved anticipating trends in software, cybersecurity, and CNI. As the topic is a sensitive one, requiring the participants to trust the researchers, we used a referral approach, asking academic and industry colleagues of the researchers for referrals. We then continued 'snowballing' further referrals from each expert interviewed.

Our criteria for approaching people were that they should have at least 5 years' expertise in a CNI discipline, plus some current professional involvement with both cybersecurity ***and*** future thinking. We also looked for diverse perspectives for the study, and therefore a range of different kinds of roles.

2.2. Data Capture

The first phase of the study consisted of one-hour interviews and was exploratory in nature, aiming to generate new insights and uncover potential future scenarios.

Although our previous work had forecasted a range of future trends in software (Weir et al., 2024), it was not clear that these trends would be the major ones for CNI. We therefore avoided bias from prompting experts with these, and instead used only open questions around the nature of CNI, likely future trends, changes in cybersecurity-related risks, and possible mitigation approaches. We piloted a first version of the survey with two colleagues knowledgeable about cybersecurity, who took the role of industry experts. Based on the trials we clarified some of the questions and added more. Appendix 1 gives the final question set.

From the analysis of the transcripts, we created an initial short report, the **round one report**, including statements describing properties of CNI, identified trends, risks and risk mitigation strategies. This is available online (Loureiro-Koechlin, Dennis, et al., 2024).

In the second stage of the study, we distributed the round one report to all participants. Each expert then completed an online questionnaire with a Likert scale of agreement to each statement in the report; and sorted the top five risks and mitigation approaches in order of their perceived priority[1]. Experts then discussed, in a half hour interview with a researcher, their reasons for anything but complete agreement with each statement and provided suggestions for improvement. We analysed the transcripts to create a **round two report**.

Of the total of 44 interviews, most were conducted online via MS Teams, recorded and transcribed automatically by the same tool. Two participants' interviews were carried out in person, with recording and transcription also carried out using a laptop running Microsoft Teams. The online questionnaire was created as a Qualtrics survey and distributed via email.

Finally, we carried out an in-person workshop to gather further insights on how best to present and use the information we had from the Delphi study. Participants were sent the round two report prior to the workshop. At the workshop, privacy restrictions prevented us recording the activities. Instead, researchers participated in the conversations and captured written notes; we also captured all artefacts and drawings created by the participants. Selected notes and drawings were then transcribed manually and analysed. A **final report** was created including the findings from the second round of the Delphi study and the recommendations from the workshop (Loureiro-Koechlin, Hunt, et al., 2024).

2.3. Data Analysis

We used both quantitative and qualitative analysis, as follows.

2.3.1. Quantitative Analysis

The quantitative data from the online survey was used in three ways.

1) The aggregated answers to the prioritisation questions were used to select the risk and mitigation approach statements with the highest numbers of votes for further analysis, and to discard the remainder. We targeted keeping at least half a dozen of each, but to choose a meaningful cut-off point in each case.

[1] *We did not ask participants to rank trends, as it was not clear on what basis they might do this.*

2) Answers to the Likert-scale questions constituted the basis for the second-round interview questions, which focused on disagreements and partial agreements with the first-round statements.

3) The aggregated responses to the Likert scale questions were then used to gauge consensus during the refinement of the statements during round 2.

2.3.2. Qualitative Analysis for Round One

Interview analysis was carried out using the tool NVivo, based on the automated transcript for each interview and referencing the audio of the interview where necessary. We used thematic analysis: transcripts from phase one interviews were analysed following an open coding approach (Strauss & Corbin, 2003). Two researchers independently coded each transcript, creating codes to categorise statements according to the concepts and issues being discussed. They met regularly to coordinate coding and compare results.

Once coding was completed, the researchers met to construct a joint 'thematic diagram' grouping codes together to form themes. They then wrote a summary of each important theme as a 'statement', referencing the corresponding coding and transcripts to ensure each statement was grounded in the transcript data. This became the round one report (Loureiro-Koechlin, Dennis, et al., 2024).

2.3.3. Qualitative Analysis for Round Two

Transcripts from phase two interviews were analysed using the same tool, this time following a confirmatory approach. Researchers assessed how the previously identified themes—trends, risks and risk mitigation strategies in round one—were discussed in the second set of transcripts. New insights were gathered for each theme and used to refine the statements.

Specifically, using NVivo we categorised the interview transcripts under codes corresponding to each first round statement. We then compiled and summarised the coded texts into bullet points in a Microsoft Word document ('the anonymised comments'). We took the statements from the round one report, removed the lower prioritised risks and mitigation statements (see section 2.3.1 item 2 above) and added the corresponding anonymised comments after each remaining statement. We used colours to group different comment subjects. We then refined the report statements to reflect those comments.

Figure 3 shows an example. The statement, 'Cascading Problems', is the text from the round one report; followed by a summary of the participants survey choices (omitting 'no opinion's); and then a precis of each notable comment from a participant. Only participants who did not 'strongly agree' would provide comments. We used highlight colours to link related comments. We then took the most relevant comments and used them as a basis to rewrite the statement. Figure 2 shows the result, with changes highlighted for illustration. From the rewritten statements we produced the round two report (Loureiro-Koechlin, Hunt, et al., 2024)

The working datasets with the round 2 survey questions plus results, extracts from participant transcripts, report statements and associated comments are available (Weir et al., 2025)

2.4. Research Ethics

Prospective participants were given participant information sheets and assured confidentiality throughout the process. Participants were asked to provide informed consent prior to their

Cascading problems: 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.

Strongly Disagree	Somewhat Disagree	Somewhat Agree	Strongly Agree
0	2	6	12

- 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.
- 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.

Figure 3: Example Statement with Phase 2 Participant Comments

inclusion in the study and were assigned anonymised identifiers. The recordings, transcripts and documentation resulting from the analysis of those transcripts were securely stored in encrypted repositories, accessible to the research team only.

The research was approved by the Lancaster University Faculty of Science and Technology Ethics Committee, reference FST-2023-3891-RECR-2.

3. Results

This section explores the results and statements created in the Delphi study.

The Round 1 interviews took place between 12 January and 11 March 2024; the Round 2 interviews between 19 April and 14 June 2024; the final workshop was on the 10 September 2024.

3.1. Recruitment Results

The process of recruiting and interviewing specialists for the first round took two months, in which we approached 40 potential candidates and recruited 22 participants. Of these, 7 were

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.

Figure 2: Resulting Statement

Table 1: Survey Participants

ID	Description (role and specialism)	Workshop	Experience (yrs)	Country	Nuclear	Energy	Telecoms	Health	Transport	Internet	Military/Defence	Emergency Services	Government	CNI	Regulation/Policy
P3	Academic specialising in cybersecurity and resilience of networked systems		26	UK	■	■	■			■				■	■
P4	Government scientist specialising in security of software systems		26	UK							■				■
P5	Government scientist specialising in security of nuclear systems		39	USA	■	■							■	■	■
P6	Academic leading major group covering cybersecurity & advanced computing		33	Aus-tria	■	■	■	■		■	■	■	■	■	■
P7	Academic leading group researching future digital resilience		24	UK		■					■			■	
P8	Human factors and cybersecurity expert working in the rail industry	Y	20	UK					■		■				
P9	Industry program director working on digital twins	Y	27	UK		■			■						■
P10	Academic leading (different) research project into future CNI risks		26	UK										■	■
P11	Independent OT cyber security consultant, working with industry and government		44	UK	■	■	■		■		■		■	■	■
P12	Academic leading cyber futures research institute		9	USA						■					■
P13	Academic, from industry, specialising in future health informatics		28	UK				■							
P14	Academic specialising in impact from research related to National Security including future cybersecurity risks		40	UK							■			■	■
P15	Academic and consultant specialising in emergency management	Y	16	UK	■			■	■			■	■	■	
P16	Academic specialising in cybercrime relating to emerging technology		30	Can ada									■		■
P17	CEO of industry consultancy specialising in OT cybersecurity		15	UK					■					■	
P18	Consultant in engineering & regulation to industry & government	Y	40	UK	■	■									■
P19	Academic expert in computer networking and resilient systems		46	UK		■	■			■			■	■	
P20	Academic specialising in international security, especially cyber warfare		13	UK	■	■	■				■			■	■
P21	Researcher specialising in cyber policy and national security		5	UK											■
P22	Author and industry consultant expert at future study and software		55	UK											■
P23	Senior academic specialising in cybersecurity, law and future tech		24	USA						■				■	■
P24	Researcher studying future resilience and sustainability		5	UK					■					■	

referrals from other participants; 10 were referrals by other colleagues of the researchers; and 5 were experts approached directly. Table 1 summarises them, including their role and country.

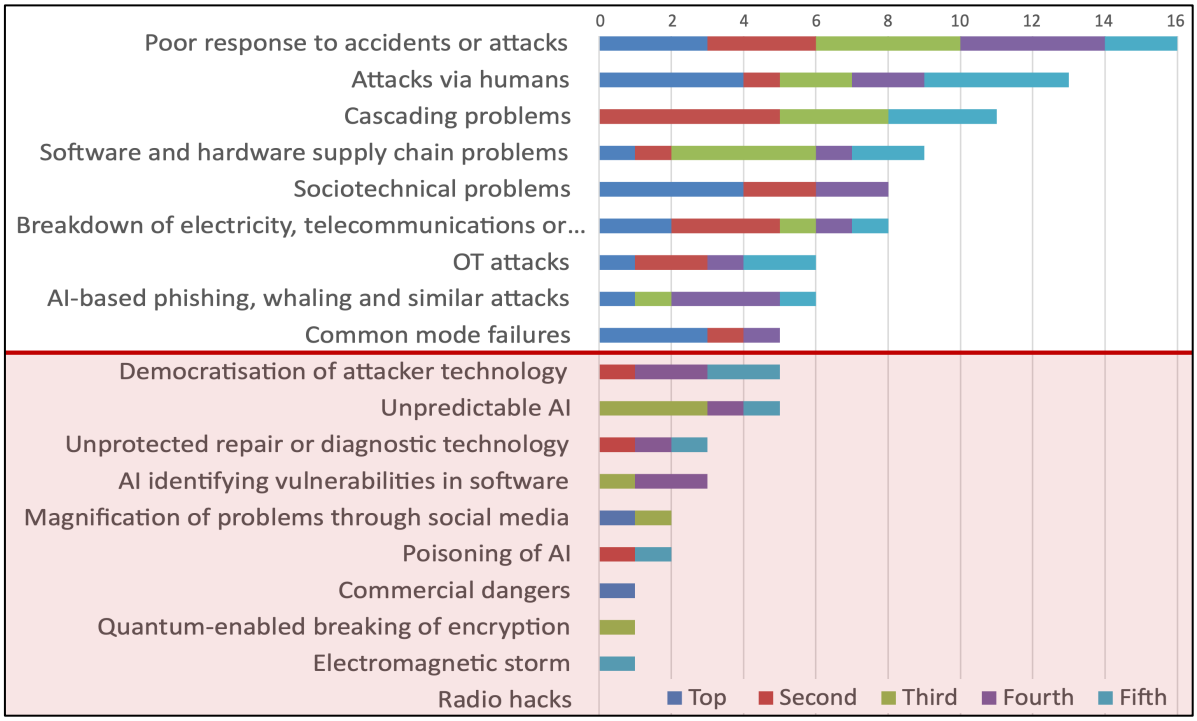

Figure 4: Selection of Highest Ranked Risks, by Number of Votes

As discussed in Section 2.1, we needed informed opinions and diverse perspectives for a credible study. Table 1 therefore also includes a description of participants' areas of expertise, and years of experience following their undergraduate degree, as confirmed with the individuals concerned. We note also that 9 of the 22 had been recent keynote speakers at substantial academic or commercial events. The last two columns indicate which participants have worked with cross-sector CNI issues, and which with government policy on CNI cybersecurity. Colours help distinguish columns. P1 and P2 were the pilot interviewees and so are omitted.

Though we focussed on the civil nuclear, communications, energy and health sectors as stated in RQ1, in practice we recruited substantial numbers of experts in military (7), transport (6) and government (6); and fewer in the health sector (4). 13 of the 22 were expert in cross-sector CNI, and 15 in government regulation and policy. The experts were mostly based in the UK (17) with four in North America and one in Austria.

The in-person workshop was attended by four of the experts, as indicated in Table 1, and three specialists in CNI futures from different areas of UK government.

3.2. Analysis Summary

The total duration of the recorded interviews was 40 hours 22 minutes, and the interview transcripts totalled 331,000 words. From the first round, the merged list of codes and analysis by the two coders generated 49 themes: 4 related to the nature of CNI, 11 related to future trends, 19 to risks, and 15 to mitigation approaches.

From the second round, we used the participants' prioritisation to identify the most important risks and mitigation approaches. Figure 4 and Figure 5 show the results. In each, colours indicate the number of participants who chose each risk as top, second, third priority, etc.; the items shaded in red were omitted from the later analysis. Fuller descriptions of each topic are in (Loureiro-Koechlin et al., 2024). Note that the 'Business as usual cybersecurity research...'

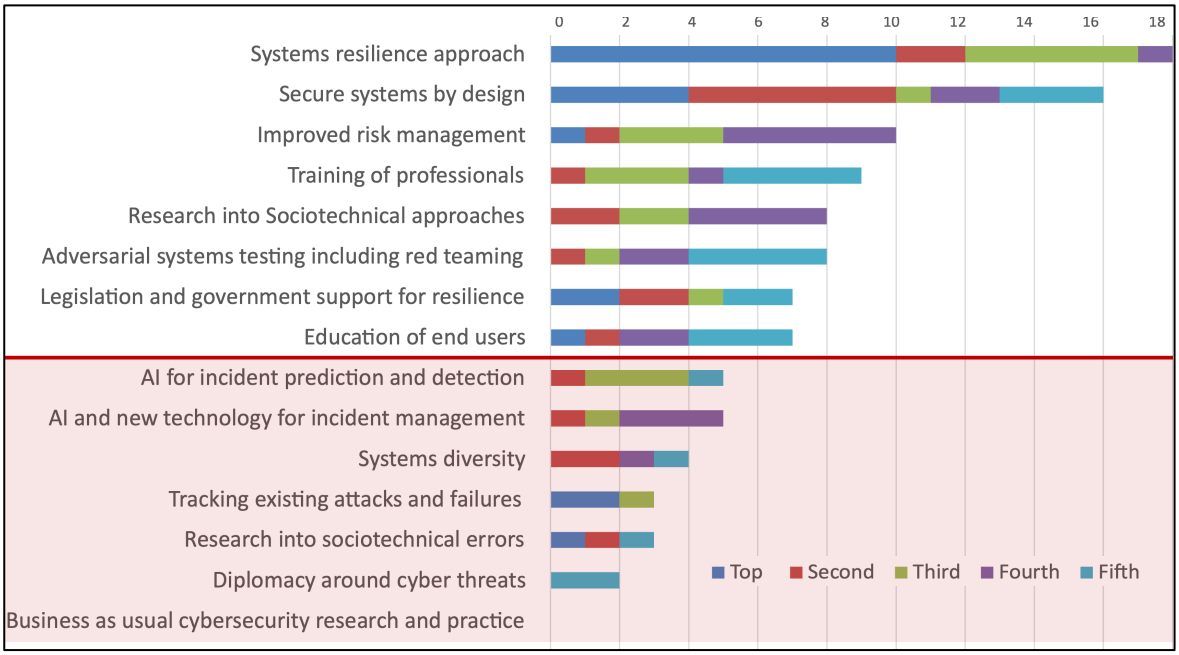

Figure 5: Selection of Highest Ranked Mitigation Approaches

statement in Figure 5 refers to current research and practice; nobody suggested cutting back on such research but many participants stated that it was insufficient to handle the new risks.

As shown, we selected the top 9 risks and 8 mitigation approaches, setting the cut-off points (red lines on both figures) to correspond to steps in average priority (see Section 2.3.1 item 1). A total of 33 statements remained. In the round 2 analysis (see Section 2.3.2), we extracted a total of 288 comments for these 33 statements and used these as a basis for rewriting each of the statements.

The following sections present the four sets of statements: 4 descriptions of CNI, 12 identified trends, 9 risks, and 8 mitigation approaches.

Workshop participants pointed out that some of the suggested mitigation approaches incorporate others; for example, human-centred cyber resilience might well involve risk assessments and training. We have therefore identified these and similar relationships during our analysis and represented them using Venn-style diagrams for each section.

To anchor the survey findings in the context of previous work, we have cited academic work related to each statement where such work was found in the literature survey. Each statement therefore includes a summary of the combined participants' views, and where appropriate, references from our literature survey. Note that the literature survey only explored future trends in the *cybersecurity of CNI*; there is other academic and commercial literature related to every topic discussed, but these are not cited here.

3.3. Expert Comments: What is CNI

The following statements summarise the participants' initial comments about the nature of CNI.

1. **Definition of CNI**: Definitions of 'Critical National Infrastructure' vary considerably (see Section 1.1). Much of CNI is in the private sector (Herrington & Aldrich, 2013), and services making up the supply chain to CNI can therefore themselves be critical (Dupont, 2013).

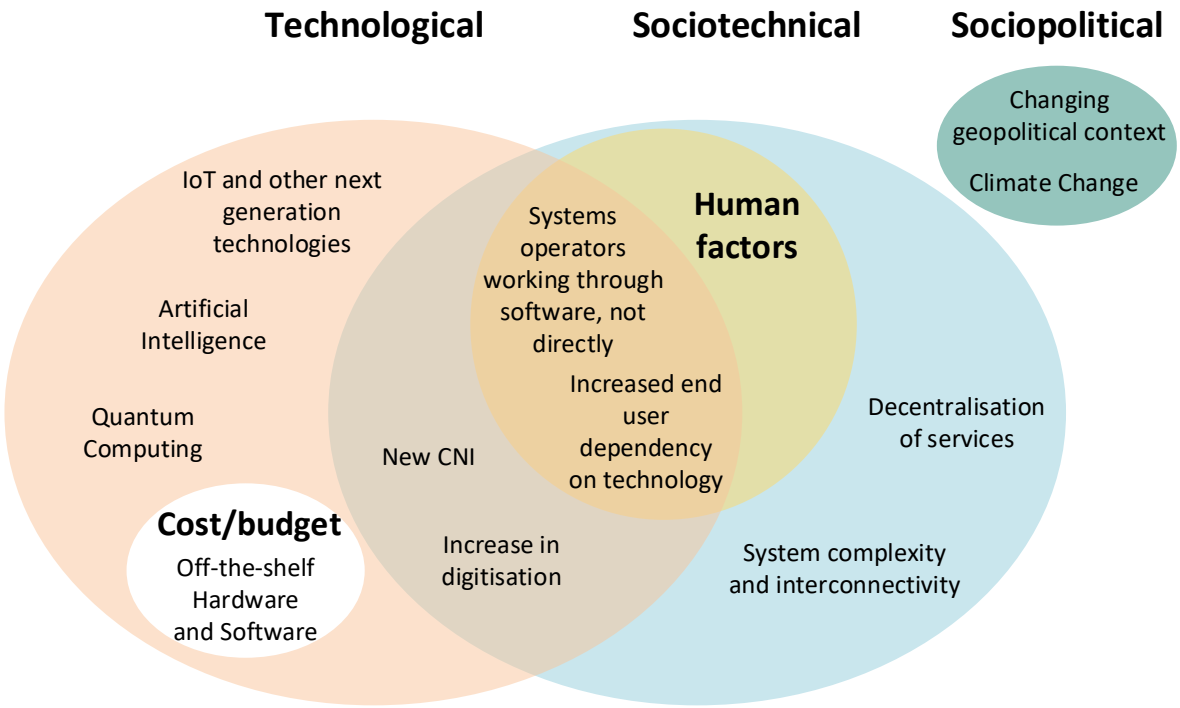

Figure 6: Overview of Fifteen Year Trends

2. **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.
3. **Commercial drivers**: CNI are operated by public and private sector organizations; commercial visions may impact technology strategies and their implementation (Rudner, 2013). However, innovation is mainly led by government discourse, often through spin-out companies led by people expert in particular CNI domains.
4. **Suppliers use regulation to coordinate response to CNI 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.

3.4. Expert Forecasts: Trends

The experts identified a range of trends affecting the potential for major incidents related to software, as shown in Figure 6. The trends are as follows.

1. **IoT and other next generation technologies**: by 2040 there will be extensive use of Internet of Things (IoT) technology: a network of physical objects embedded with sensors and actuators that connect and exchange data with systems over the internet (Adegbite et al., 2023; Preston et al., 2022; Raban & Hauptman, 2018; Viganò et al., 2020). These will be supported by Cloud internet processing, and often 'Digital Twins' (Bhamare et al., 2020)—virtual representations of physical systems for monitoring, simulation, and analysis. 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.

2. **System complexity and interconnectivity**: by 2040, CNI software systems will have increasingly complex architectures and increasing connections to other systems, though less so in highly regulated sectors (Adegbite et al., 2023; Bhamare et al., 2020). This will make it more difficult to understand the complex sociotechnical interactions involved—the interplay between humans and technology within each system—and will in some cases make systems more vulnerable to human error and to attacks.

3. **Increase in digitisation**: Towards 2040, most infrastructure will become software-controlled, to simplify control, increase efficiencies, decrease costs, and provide data accessibility (Scholz et al., 2022).

4. **Decentralisation of services**: Towards 2040, digitisation will enable the distribution of CNI functions and services away from a central point to various, often remote, locations. Remote communications, wireless and radio technologies will allow the dispersal of functions (Nazari & Musilek, 2023), like electricity generation, perhaps including nuclear in the form of Small Nuclear Reactors. Centralised control will still be the default in most cases.

5. **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.

6. **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 (Scholz et al., 2022).

7. **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.

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

9. **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 (Tahirkheli et al., 2021; Vaughan-Nichols, 2023). Although, since the date of the study the UK has defined data centres to be CNI (Gov.uk, 2024) this trend refers to cloud software services rather than hardware.

10. **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 (Blauth et al., 2022; Brundage et al., 2018; Nazari & Musilek, 2023; Raban & Hauptman, 2018).

11. **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 Artificial Intelligence (AI) techniques. Quantum breaking of cryptographic encryption might be possible then, though easily mitigated by algorithm changes (Adegbite et al., 2023). Quantum techniques for secure communication will be used in some cases.

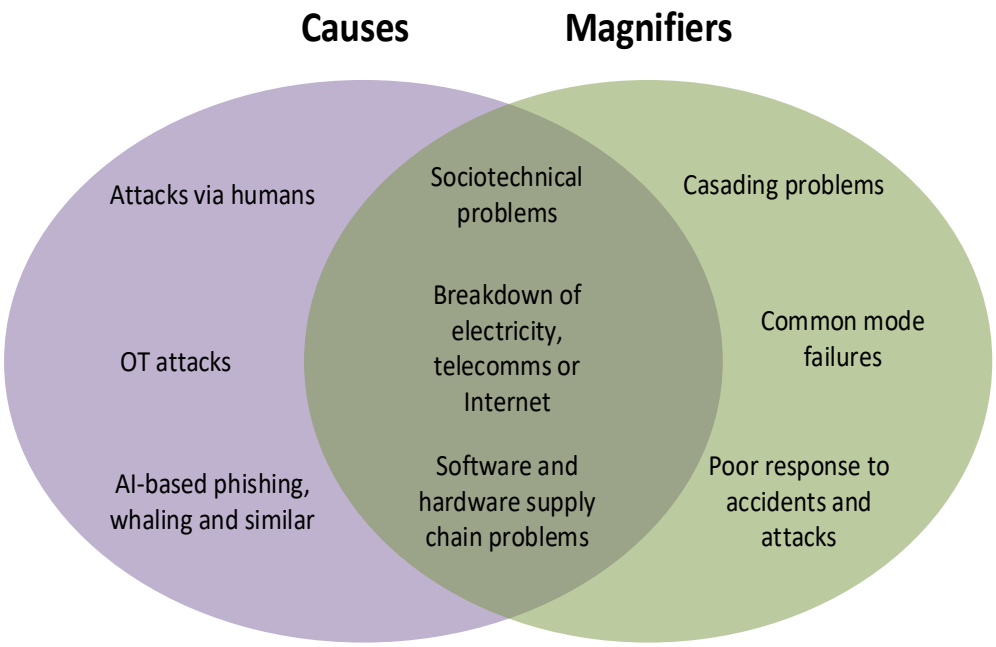

Figure 7: Identified Risks

12. **Off-the-shelf hardware and software**: Towards 2040, some CNI systems will increasingly be made from off-the-shelf hardware and software components. This brings benefits in cost and sometimes reliability but will bring risks where they are not built to a high enough standard (Preston et al., 2022; Raban & Hauptman, 2018). Many CNI operators will still prefer to develop bespoke systems or to strengthen their off-the-shelf components.

3.5. 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. Figure 7 illustrates the risks identified by the study participants, distinguishing primary 'causes' of incidents from subsequent 'magnifiers' of an incident's impact. The following sections describe each risk.

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:

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

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

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

2. **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 (Blauth et al., 2022; Johnson, 2019) and make it easier to automate attacks (Brundage et al., 2018).

3. **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 (Deibert & Rohozinski, 2010). The complexity of systems will make it difficult to identify such vulnerabilities in advance.
4. **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 (Sobb et al., 2020). 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.
5. **Sociotechnical errors**: 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—as happened, for example, in the Three Mile Island and Chernobyl incidents.
6. **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.
7. **OT attacks**: Operational Technology (OT)—the systems that monitor and control physical processes, particularly in industries like manufacturing, energy, and utilities—used to be relatively safe from cyberattack 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 (Murray et al., 2017).
8. **AI-based phishing, whaling and similar attacks**: Towards 2040, generative AI will be widely used in cyber-attacks where individuals are tricked into divulging confidential information or installing malware. 'Whaling', which targets high-profile individuals, will be particularly affected (Blauth et al., 2022; Johnson, 2019).
9. **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.

3.6. Expert Suggestions: Mitigation Strategies

Our experts suggested a range of complementary approaches to address the future risks they identified, as illustrated in Figure 8. Such 'mitigation approaches' address and reduce the wider

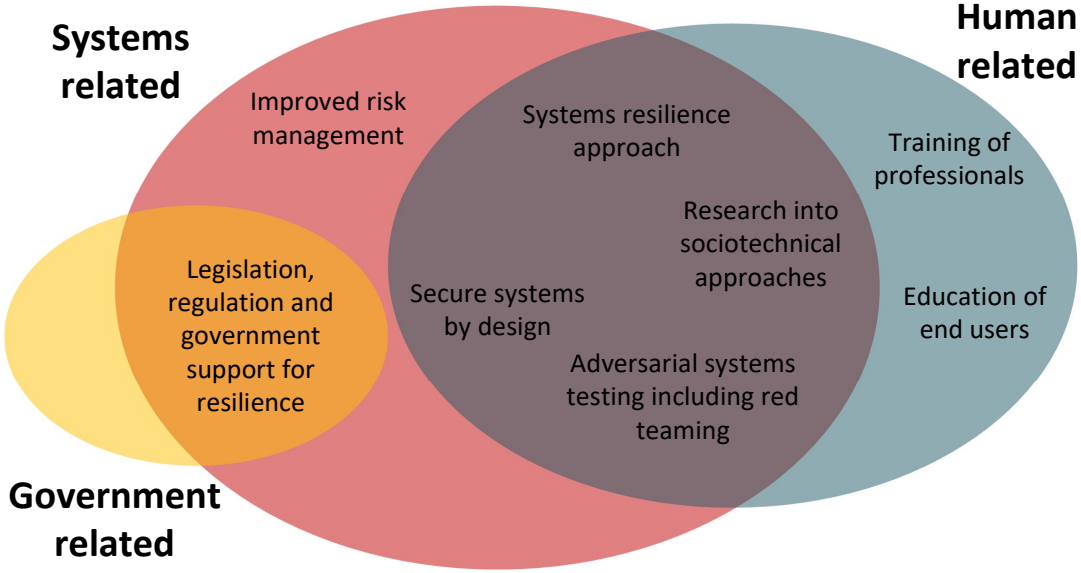

Figure 8: Mitigation Strategies

problem in addition to improving defences and the response to incidents. The following sections explore each mitigation suggested.

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.

2. **Secure systems by design (SSBD)**: Also known as Security by Design, SSBD incorporates systems security, privacy and safety analysis—including human interaction analysis—from the earliest stages of design in creating and modifying software systems rather than later in the development cycle. By focusing on individual products and components, SSBD delivers layers of security, provides a path for upgrades, and can be applied to enhancements to existing systems.

3. **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.

4. **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.

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

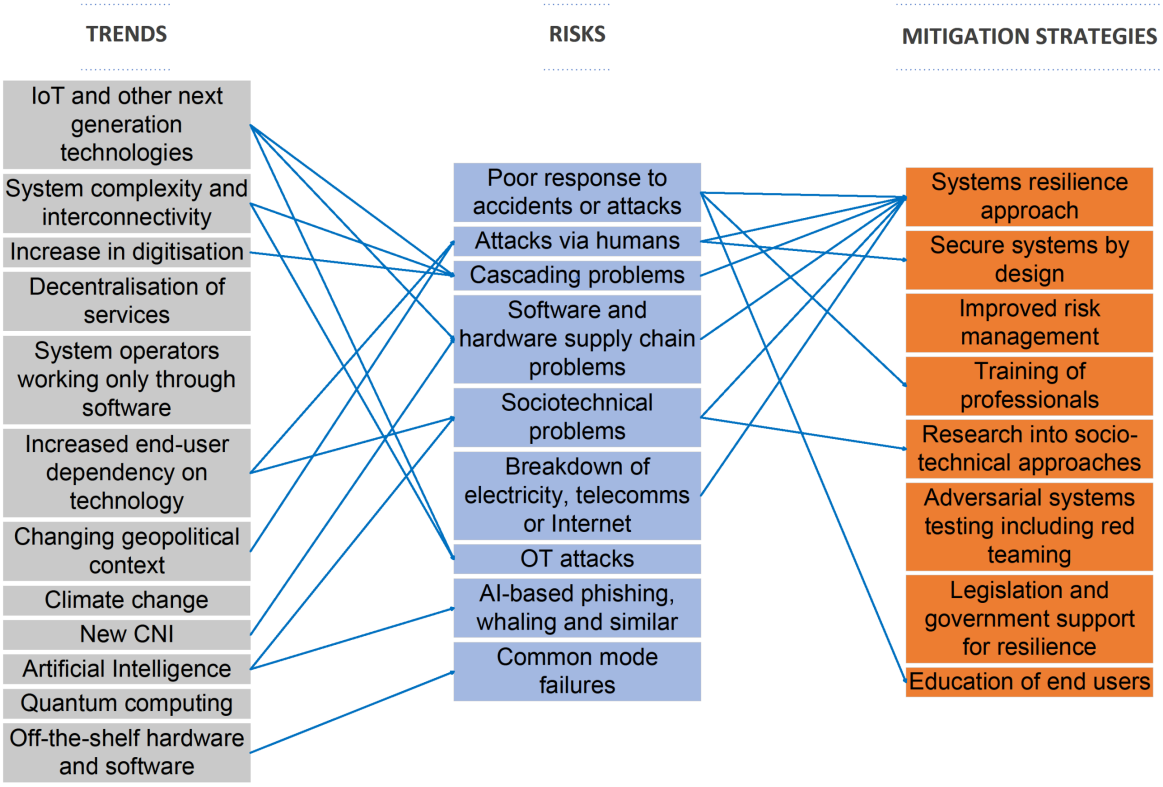

Figure 9: Derivation of Risks from Trends, and Mitigation Strategies from Risks

6. **Adversarial systems testing including red teaming**: While 'Penetration Testing' only explores weaknesses in the software, 'Red Teaming' involves cybersecurity experts simulating attacks on the whole system, including human users and support staff. Techniques include both ethical hacking, and social engineering approaches.

7. **Legislation, regulation and government support for resilience:** to motivate organisations to invest in systems resilience, secure by design approaches and adversarial systems testing. This is important given most CNI is privately managed (Viganò et al., 2020). Effective tools tend to be regulations supported by laws, and industry standards and implementation guides.

8. **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.

3.7. Relationship between Statements

Figure 9 is derived from the outputs of the in-person workshop. It shows the relationship between the statements in the previous sections: showing how trends lead to risks, which in turn can be addressed by mitigation strategies. The data came from an exercise done independently in three groups of experts at the workshop; the figure shows only the connections identified by at least two of the groups.

As shown, there was no consensus on legislation as a primary cure for the major issues identified; instead, to our surprise, there was a strong emphasis on the human centred approaches, including human-centred analysis into resilience, training, and sociotechnical research.

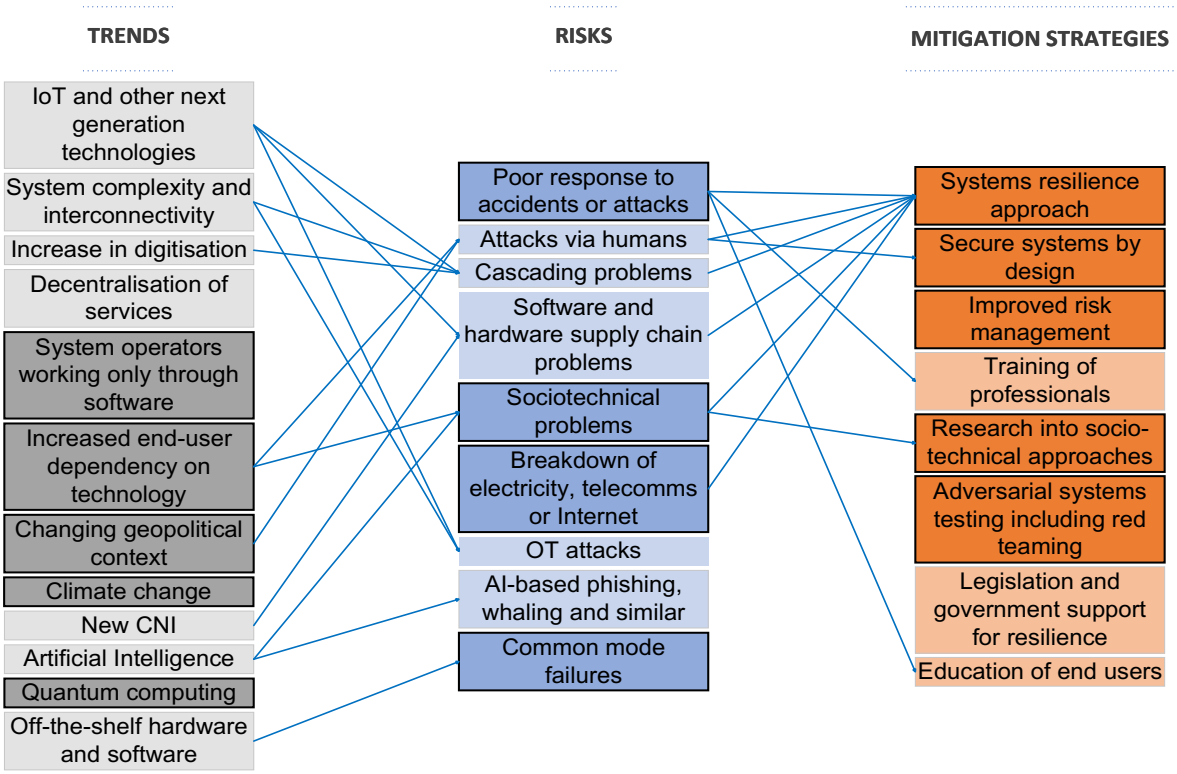

Figure 10: Relationships, showing Topics Found and Not Found in Prior Literature

4. Discussion

This section discusses the results, comparing them with prior work and exploring two key recommendations in more detail.

4.1. Comparison with Prior Work

Naturally, all the issues raised by our survey participants have been explored in other academic contexts than the future of CNI cybersecurity. However, as shown in Section 3.5, many of the new risks raised are relatively new to *this context* and we have not found corresponding discussion in the academic literature. Specifically, the research question spans several academic domains—future studies, cybersecurity, management, software engineering, sociology, for example—and many aspects have been studied only in their specific domains and with no consideration of the other aspects of our research question RQ1. Where we have found such references in the context of CNI security, they were indicated in the corresponding descriptions in Section 3.5. Figure 10 builds on Figure 9 by highlighting which aspects are new to the cybersecurity dialogue: bold colours are statements with no previous discussion in the cybersecurity futures literature we found.

4.2. Relationships between Trends, Risks and Mitigation Approaches

In Figure 10, we observe two risks that apparently do not derive from any of the trends identifed by the experts: *Poor response to attacks and accidents*; and *Breakdown of electricity, telecomms or internet*. Based on the workshop discussions, this reflects that *Poor response to attacks and accidents* is actually a problem exacerbated by all of the trends, rather than associated with any specific one. It is less clear why *Breakdown of electricity, telecomms or*

internet had no associated trends; given the current typical breakdown causes of weather, grid instability and equipment failure (Waseem & Manshadi, 2020) we identify climate change and system connectivity as candidates.

Similarly, there were no specific risks for which *Improved risk management, Adversarial systems testing,* or *Legislation and government support for resilience* were identified as mitigations. Again, as each of these can to some extent contribute to addressing any of the risks listed, we can deduce that the reason was a lack of specificity rather than a lack of need.

The lack of prioritised mitigation approaches for the lowest three risks might be concerning, but probably reflects simply that 'business as usual' cybersecurity research is already addressing them.

4.3. New Trends and Risks

As shown, three of the newly identified trends belong in the wider context of CNI systems: *Changing geopolitical context*; *Climate change* and *Quantum computing*. These might easily be considered outside the scope of typical earlier computer futures work. However, the other two newly identified trends are human-centric: *System operators working only through software*, and *Increased end-user dependency on technology.* Adding these human-centric trends to the future study opened the scope towards more human centred risks as well.

Generative AI was widely hyped at the time of the survey, and as researchers we had expected AI risks to predominate. This was not the case. Virtually every participant discussed AI risks, but only AI-based phishing and whaling were seen as a primary concern, and as Figure 10 shows, even those were not the most pressing. The consensus appeared to be that new research and appropriate new regulation will mitigate most AI threats.

The major risk, to our surprise as researchers, was outside the scope of much of cybersecurity research: *Poor response to accidents and attacks*. Several further risks had not featured significantly in the literature, including *Common mode failures*, where lack of diversity in hardware and software means that a single attack or problem can have huge impacts; and *Sociotechnical problems*, where non-malicious human choices can cause disasters due to human factors issues in the system design.

4.4. Exploring the Mitigation Approaches

Two of the mitigation approaches were prioritised in the discussions in the in-person workshop: *[Human-centred] systems resilience approach*, and *Legislation, regulation and government support for resilience.* Accordingly, we explore these further here.

4.4.1. Human-Centred Systems Resilience Approach

While cyber resilience as a concept is definitely a subject for research, and even commands an academic conference on the subject, unfortunately the phrase appears to be taken by the academic cybersecurity community as referring only to cybersecurity attack detection and defence techniques, along with studying humans as possible threat vectors ("CSR Conference," 2023). However, the surveyed experts had a very different view of cyber resilience, starting with the assumption that some attacks will be successful. Their concept of cyber resilience includes systems thinking, incident planning, red teaming, redundancy in provision, design for gradual degradation and the enforcement of systems diversity (Section 3.6).

Table 2: Participant Statements about Resilience

- *[I work] mostly on cyber resilience … because I think cybersecurity … is an impossible objective to achieve with these new technologies and risks (P16)*
- *[Cyber resilience] is about systems thinking: … systems engineering, software engineering, … but also human elements as well (P18)*
- *We need a mentality change from trying … to prevent things, to accepting bad things will happen. But then we need mechanisms to respond fast. (P7)*
- *So you end up with systems … designed to be graceful in their degradation. (P11)*
- *It's important to use… other disciplines to think about the risks involved. Resilience comes at a cost, because we're talking about adding redundant components and paths. (P19)*
- *The key thing is that it's a systems problem. And we will not be able to fix any of these things until we think of them as systems problems. (P23)*
- *Actor Network Theory is a helpful way of looking at [a systems approach]: each scale of a 'system' … is made up of tiny smaller systems. (P15)*
- *It's important to use people from other disciplines to think about the risks involved. … There are [also] some [relevant] design ideas: decoupling error detection and correction; graceful failure; duplication; … diversification. (P19)*

More specifically, Table 2 provides edited quotations from the survey participants about their understanding of the kinds of resilience required. Text in brackets is added for context; ellipses indicate omitted text. The statements make it clear that meaningful research about human-centred cyber resilience will require a transdisciplinary approach (Wickson et al., 2006), incorporating systems thinking, ergonomics, management science, sociology and psychology as well as technical cybersecurity (Ungar, 2021).

4.4.2. Legislation, Regulation and Government Support for Resilience

Participants were clear that legislation had a role to play, especially given that much CNI is in private ownership and that commercial interests may not have the same incentive for disaster prevention as the communities they serve. However, they were also clear that it was not the whole answer. The condensed extracts from interviews and the workshop in Table 3 give an indication of the range of comments about legislation. The comments make it clear that much of the work will be in standards and regulations, but that there is a need for legislative change to handle specific problems, especially the lack of any equivalent of product liability for software services (Howells & Weatherill, 2017).

4.5. Relationship to Topical Research and Concerns

One surprising aspect of the analysis Figure 4 in Section 3.2 was the apparently low priority given by survey participants to several of the most exciting and challenging new areas of research and technology strategy: unpredictable AI, AI identifying vulnerabilities in software, poisoning of AI, and quantum-enabled breaking of encryption. Another related surprise was the low priority apparently given to the mitigation 'Business as Usual Cybersecurity', a catch-all term for existing work being done to address current threats.

The explanation is in the context of the survey: our questions (Appendix 1) related to **future changes in the computing landscape**. Nobody suggested that the concern around AI was understated, nor underestimated the impact of quantum breaking of encryption—and certainly nobody hinted at abandoning 'business as usual' cybersecurity practice. In the context of the

Table 3: Participant Statements about Legislation

- *[Companies in highly regulated sectors] coordinate their spending through agreement on regulation, so they agree standards rather than each do their own thing. (P19)*
- I *think the UK is probably …five or 10 years ahead of the pack of most countries in terms of legislation for resilience. Well, it's not legislation; it's regulation for resilience. (P16)*
- *[We need] legislation and government support for resilience to address the lack of commercial interest. Government support for resilience means that you have to invest in testing, and you have to invest in systems resilience and the security by design process. (P20)*
- *Government support for resilience is important and legislation is important, but the taxpayer can't do everything; … it is a business's job to [become resilient]. (P4)*
- *We need legal innovation … that encourages resilience when there is an attack that can be overcome. We [also need] a [legislative] regime for dealing with … software tied to services rather than products. (P23).*
- *Legislation itself is not a mitigation but a vehicle to help implement mitigations (Workshop participant)*
- *The most important tools are the regulations and standards beneath the overarching laws. We should aim to modify existing regulations rather than create new ones; promote management regulations over technical ones; and establish unified standards for industry best practices (Workshop participant)*

survey discussions these are all taken as a given, **including the new research and policy work around AI and quantum computing**.

What the survey participants stressed was that, given this context, the largely unconsidered risks associated with **poor responses to cyber accidents and attacks** have become a dominant problem.

4.6. Limitations

As with any study of this kind, this survey has limitations. First, with over 75% of the participants based in the UK (Section 3.1), the conclusions can only represent expert opinion on Critical National Infrastructure in that country. While all the trends and risks identified are global in nature (Sections 3.4, 3.5), the identified risk priorities and context for the mitigation approaches (Section 3.6) will depend on local factors and so should be treated with caution for other countries.

Of the 13 sectors of Critical National Infrastructure, plus Internet, only 9 sectors are represented by the participants (Table 1 in Section 3); whilst none of the trends or risks identified are specific to those sectors, it is possible that experts from other sectors would have different forecasts, concerns and priorities.

Recruitment using referrals may be the only practical way to recruit participants in such a sensitive topic area (Section 2.1), but would lead to bias if a high proportion of participants belonged to a particular community of practice. To mitigate this, we used many sources of referral (Section 3.1) and approached some candidate participants directly.

The compression of around 200,000 words of the round one interviews into a 2,000-word Round one report necessitated omitting a huge amount of data; it is possible that one or more important themes may have been omitted despite the care taken by the researchers. Against that possibility, we note that these are *forecasts*, and so there is no ground truth; moreover, the

omission of a theme mentioned in the interviews would not invalidate the themes which *have been* included. So, such an omission would not invalidate the forecasts in this report.

Given that these are forecasts, readers should be careful to make allowance for the future unfolding in a way not expected by the survey participants, which will become increasingly likely with passing time.

5. Conclusion

The findings from this Delphi study offer original perspectives on technological risks concerning CNI software, contributing new insights to the ongoing discourse on cybersecurity. The study included multiple participants from eight of the thirteen UK CNI sectors (Section 3.1), and from a suggested new CNI sector, Internet (Section 3.4 item 9).

Considering *RQ1 What effect may change in the nature and use of software systems between now and 2040 have on the potential for major incidents related to UK Critical National Infrastructure…,* the findings contrasted with existing academic literature (Section 4.1). Specifically, the participants prioritised a range of new risks in the relationships between humans and the software involved with CNI (Section 3.5), notably:

- **1. Poor response to accidents or attacks**, where the operator and management responses to incidents contributes to the impact; and
- **5. Sociotechnical errors**: where human factors issues lead to increasing disruptions even when all the participants are working in good faith.

In response to *RQ2 What actions can we as a society take now to address the resulting risks,* the participants proposed two particular research and societal approaches to address these and other likely issues (Section 3.6):

- **1. [Human-centred] systems resilience approach**, involving human factors and systems based transdisciplinary approaches, and
- **7. Legislation, regulation and government support for resilience,** which will be mainly in regulation and standards, but may require legislation support, especially around the lack of any equivalent of product liability for software services.

We can summarise this conclusion as:

> Increasing risks in many areas, from cascading failures, through human-centred issues to AI, will all contribute to systems that ***will*** occasionally misbehave in ways that are potentially very damaging. So, rather than focus only on perfect solutions we need to prepare human centred approaches and software to reduce that damage: human centred systems resilience.

5.1. Next steps

We suggest future transdisciplinary research on ways and regulatory support to improve organisations' human-centred systems cyber resilience. We anticipate such research to involve cybersecurity, software engineering, management, ergonomics, psychology, sociology and law. Possible approaches to this research might include:

- Interviews and case studies on effective service resilience in the cyber domain;
- Attributes and changes to Security Operations Centres to support wider resilience;
- System functionality to best support resilience in different situations;
- Adapting existing resilience and disaster planning research to software and cyber;
- Policy proposals for regulation and insurance governance; and
- Metrics to identify targets for human-centred cyber resilience.

Adopting these approaches offers a valuable way forward for the future.

6. Acknowledgement

This research was funded by the UK North West Partnership for Security and Trust, which is funded through the UK Government Communication Headquarters (GCHQ). The funding arrangements required this paper to be reviewed to ensure that its contents did not violate the UK Official Secrets Act nor disclose sensitive, classified or personal information.

The funders, however, had no role in study design; in the collection, analysis and interpretation of data; in the writing of the report; nor in the decision to submit the article for publication.

6.1. Declaration of Generative AI in the Writing Process

During the preparation of this work an author used ChatGPT to review the phrasing of the abstract and to suggest keywords. After using this service, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

7. References

Adegbite, A. O., Akinwolemiwa, D. I., Uwaoma, P. U., Kaggwa, S., Akindote, O. J., & Dawodu, S. O. (2023). Review of Cybersecurity Strategies in Protecting National Infrastructure: Perspectives from the USA. *Computer Science & IT Research Journal*, *4*(3), 200–219.

Beiderbeck, D., Frevel, N., von der Gracht, H. A., Schmidt, S. L., & Schweitzer, V. M. (2021a). Preparing, Conducting, and Analyzing Delphi Surveys: Cross-Disciplinary Practices, New Directions, and Advancements. *MethodsX*, *8*, 101401. https://doi.org/10.1016/j.mex.2021.101401

Beiderbeck, D., Frevel, N., von der Gracht, H. A., Schmidt, S. L., & Schweitzer, V. M. (2021b). Preparing, Conducting, and Analyzing Delphi Surveys: Cross-Disciplinary Practices, New Directions, and Advancements. *MethodsX*, *8*, 101401. https://doi.org/10.1016/j.mex.2021.101401

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for Industrial Control Systems: A Survey. *Computers & Security*, *89*, 101677. https://doi.org/https://doi.org/10.1016/j.cose.2019.101677

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI. *IEEE Access*, *10*, 77110–77122. https://doi.org/10.1109/ACCESS.2022.3191790

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H. S., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., HÉigeartaigh, S. Ó., Beard, S., Belfield, H., Farquhar, S., … Amodei, D. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *CoRR*, *abs/1802.0*. http://arxiv.org/abs/1802.07228

CISA. (2024). *Critical Infrastructure Security and Resilience*. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

Collins, R. (1999). *Macrohistory: Essays in Sociology of the Long Run*. Stanford University Press.

Coyle, G. (1997). The Nature and Value of Futures Studies or Do Futures Have a Future? *Futures*, *29*(1), 77–93. https://doi.org/10.1016/S0016-3287(96)00067-5

CSR Conference. (2023). *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, xiii–xiv. https://doi.org/10.1109/CSR57506.2023.10224987

Deibert, R. J., & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, *4*(1), 15–32. https://doi.org/10.1111/j.1749-5687.2009.00088.x

Dupont, B. (2013). Cybersecurity Futures: How Can We Regulate Emergent Risks? *Technology Innovation Management Review*, *3*, 6–11. https://doi.org/http://doi.org/10.22215/timreview/700

Gov.uk. (2024). *Data centres to be given massive boost and protections from cyber criminals and IT blackouts - GOV.UK*. https://www.gov.uk/government/news/data-centres-to-be-given-massive-boost-and-protections-from-cyber-criminals-and-it-blackouts?utm_source=chatgpt.com

Herrington, L., & Aldrich, R. (2013). The Future of Cyber-Resilience in an Age of Global Complexity. *Politics*, *33*(4), 299–310. https://doi.org/10.1111/1467-9256.12035

Howells, G., & Weatherill, S. (2017). *Consumer Protection Law: Second Edition* (2nd ed.). Taylor and Francis.

Johnson, J. (2019). Artificial Intelligence & Future Warfare: Implications for International Security. *Defense & Security Analysis*, *35*(2), 147–169. https://doi.org/10.1080/14751798.2019.1600800

Loureiro-Koechlin, C., Dennis, L., & Weir, C. (2024). *Software Risks for Critical Infrastructure towards 2040: Round 1 Report*. Zenodo. https://doi.org/10.5281/zenodo.13255282

Loureiro-Koechlin, C., Hunt, L., Dennis, L., & Weir, C. (2024). *Software Risks for Critical Infrastructure towards 2040: Expert Forecasts - Final Report*. Zenodo. https://doi.org/10.5281/zenodo.13898514

Murray, G., Johnstone, M. N., & Valli, C. (2017). The Convergence of IT and OT in Critical Infrastructure. *Australian Information Security Management Conference*, 149–155. https://doi.org/10.4225/75/5a84f7b595b4e

Nazari, Z., & Musilek, P. (2023). Impact of Digital Transformation on the Energy Sector: A Review. *Algorithms*, *16*(4), 211.

NPSA. (n.d.). *UK Critical National Infrastructure*. Retrieved March 5, 2024, from https://www.npsa.gov.uk/critical-national-infrastructure-0

Preston, J., Bertolli, M., Eggers, S., McKenzie, P. L., Thorsen, D., Haack, J., Thomas, K., Burke, L. M., & Rosa De Jesus, D. A. (2022). *Emerging Threats and Technology Investigation: Industrial Internet of Things - Risk and Mitigation for Nuclear Infrastructure*. https://doi.org/10.2172/1893157

Raban, Y., & Hauptman, A. (2018). Foresight of Cyber Security Threat Drivers and Affecting Technologies. *Foresight*, *20*(4), 353–363. https://doi.org/10.1108/FS-02-2018-0020

Rhyne, R. (1981). Whole-Pattern Futures Projection, Using Field Anomaly Relaxation. *Technological Forecasting and Social Change*, *19*(4), 331–360. https://doi.org/10.1016/0040-1625(81)90005-6

Rudner, M. (2013). Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. *International Journal of Intelligence and CounterIntelligences*, *2*(3), 453–481. https://doi.org/10.1080/08850607.2013.780552

Scholz, C., Schauer, S., & Latzenhofer, M. (2022). The Emergence of New Critical Infrastructures. Is the COVID-19 Pandemic Shifting Our Perspective on What Critical Infrastructures Are? *International Journal of Disaster Risk Reduction*, *83*, 103419. https://doi.org/https://doi.org/10.1016/j.ijdrr.2022.103419

Slaughter, R. A. (1998). Futures Studies as an Intellectual and Applied Discipline. *The American Behavioral Scientist*, *42*(3). https://doi.org/10.1177/0002764298042003008

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. *Electronics*, *9*(11), 1864. https://doi.org/10.3390/electronics9111864

Strauss, A. L., & Corbin, J. (2003). Open Coding. In *Social Research Methods: A Reader* (pp. 303–306). Routledge, London, UK.

Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., Ayub, N., & Kim, K.-I. (2021). A Survey on Modern Cloud Computing Security Over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. *Electronics*, *10*(15), 1811.

UK Government. (1948). *Civil Defence Act 1948*. https://www.legislation.gov.uk/ukpga/Geo6/12-13-14/5/contents/enacted

UK Government. (2023). *National Risk Register 2023 Edition*. https://access-national-risk-register.service.cabinetoffice.gov.uk/

Ungar, M. (2021). *Multisystemic Resilience: Adaptation and Transformation in Contexts of Change*. OUP.

Vaughan-Nichols, S. (2023). *The cloud is critical infrastructure – here's what that really means*. Fierce Network. https://www.fierce-network.com/multi-cloud/cloud-critical-infrastructure-heres-what-really-means

Viganò, E., Loi, M., & Yaghmaei, E. (2020). Cybersecurity of Critical Infrastructure. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The Ethics of Cybersecurity* (pp. 157–177). Springer International Publishing. https://doi.org/10.1007/978-3-030-29053-5_8

Waseem, M., & Manshadi, S. D. (2020). Electricity Grid Resilience amid Various Natural Disasters: Challenges and Solutions. *The Electricity Journal*, *33*(10), 106864. https://doi.org/10.1016/J.TEJ.2020.106864

Weir, C., Dyson, A., Jogunola, O., Dennis, L., & Paxton-Fear, K. (2024). Interlinked Computing in 2040: Safety, Truth, Ownership, and Accountability. *Computer*, *57*(1), 59–68. https://doi.org/10.1109/MC.2023.3318377

Weir, C., Loureiro-Koechlin, C., & Dennis, L. (2025). *Software Risks for Critical Infrastructure towards 2040: Delphi Study Research Dataset*. https://doi.org/10.5281/zenodo.14164736

Wickson, F., Carew, A. L., & Russell, A. W. (2006). Transdisciplinary Research: Characteristics, Quandaries and Quality. *Futures*, *38*(9), 1046–1059. https://doi.org/10.1016/j.futures.2006.02.011

8. Appendix 1: Round 1 Interview Questions

The following are the questions used in the Round 1 interviews. Items *[in italics in square brackets]* are guidelines for the interviewer.

Q: In this project, we are looking to explore the future impact of changes in computing technology on Critical National Infrastructure: changes such as Artificial Intelligence, increased interconnection, Internet of Things, quantum etc.

Q: We're looking to discover relevant trends, how those trends may develop and lead to risks in the next fifteen or so years towards 2040, and what we might do to address them. So, to start…

Context:

Q: Briefly, what is your role?

Q: And what is your involvement with Critical National Infrastructure at present?

Technology:

Q: What computing technologies or trends do you see as the biggest game changers being implemented in your area right now?

Q: How do you see them evolving and changing your sector in the next 15 years? *[Prompt for examples, if appropriate]*

Concerns:

Q: What are your worries about major incidents that keep you awake at night, and how will the changes affect them?

Q: What combinations of incidents and errors could really mess up things in your sector?

Q: That sounds great. Can we make it more concrete – give an example of a possible series of incidents that could lead to that?

Q: In an earlier stage in this project, we identified a few problem trends for technology in general. If we take each in turn, can I ask you how you feel that trend will apply in your sector/work to Critical National Infrastructure? *[Probably only do first 2]*

1. *[Not for single sector expert]* More forms of infrastructure are becoming critical, such as e-retail (under COVID) and cloud computing services.
2. AI will make it difficult to distinguish truth from fiction due to misinformation and biased data.
3. As systems become more complex and interconnected, people cannot distinguish accidents from malicious activity.
4. The complexity of connected systems will lead to more accidents and catastrophic failure modes.
5. AI-driven cyber-attacks will lead to a malware and anti-malware arms race.

[Go back to the examples question if any sound like new scenarios]

Possible solutions:

Q: So you've described several hair raising worries. Where do you think we should be putting our effort to address or prevent them?

[First worry, if appropriate]

[Worry 2, if appropriate, etc.]

Taking it forward:

Thank you – that was very helpful.

Q: What documents or reports do you think would be useful for us to read?

Q: What conferences or events in this area would be useful for gaining more information?

Q: Who else might have interesting views on this who might be interested to talk to us?

Q: We'll be pulling together a summary and circulating it by *[early March]*. Please may I approach you to set up a further interview then?