Summary Report

Roundtable Discussion: Building Resilience in the UK's Electromagnetic Environment

5th & 6th February 2024
In-person workshop
Cranfield University

Dr Fabian Steinmann, Cranfield University

Steinmann, F. & Riley-Smith, T. (2024). *Summary Report - Roundtable Discussion: Building Resilience in the UK's Electromagnetic Environment*. https://www.cranfield.ac.uk/~/media/files/summary-report-roundtable-discussion-building-resilience-in-the-uks-electromagnetic-environment.ashx

Table of Contents

List of Abbreviations

CNI	Critical National Infrastructure
DAFNI	Data & Analytics Facility for National Infrastructure
DEW	Directed Energy Weapons
EME	Electromagnetic Environment
EMP	Electromagnetic Pulse
EW	Electronic Warfare
GNSS	Global Navigation Satellite System
LRF	Local Resilience Forum
NRR	National Risk Register
NSEC	Network for Security Excellence and Collaboration
PNT	Positioning, Navigation, and Timing
RAEng	Royal Academy of Engineering
RF	Radio Frequency

Preface

This is an important Report, not only because the subject matter is of critical significance, but also because of the range and quality of policy-makers, practitioners and researchers who have contributed to it.

These pages drive home the scale of the challenge, with recommendations for strengthening the UK's resilience to threats to its electromagnetic environment.

This is not a case of "what if?" but "when?" One day, severe space weather could lead to a global catastrophe; but there are also growing opportunities for localised disruption to be inflicted upon our Critical National Infrastructure by bad actors.

Credit for this initiative must go to Simon Harwood at Leonardo UK. Simon's past life – as Director of Security at Cranfield – left him well-placed to understand the contribution that research can make to illuminate the darkest of corners and to identify opportunities to resolve the most wicked of problems. He recognised the need to investigate the state of our electromagnetic resilience and it was his idea to sponsor this roundtable.

Thanks are also due to Cranfield University (Professor David Denyer and Dr Annette Southgate among others) for responding positively to this proposal, and for putting arrangements in place to deliver such a successful event.

Electromagnetic Resilience feels like an archetypical "elephant in the room". It is a substantive threat that sits on the periphery of our vision: partly because of uncertainty as to when it might "go rogue"; partly because the worst impact – from a future Carrington Event – is almost too terrible to contemplate; and partly because the cost of mitigation must compete with a long list of pressing short-term challenges.

This Report aims to prompt discussion and action on strengthening electromagnetic resilience. This is not happening in a vacuum. Several significant papers have been written over recent years, such as the RAEng and New Zealand Government reports featured below. In 2021, the UK Government published its *Severe Space Weather Preparedness Strategy*; and in October

2023 it announced a new policy framework for greater Position, Navigation, and Timing (PNT) Resilience, accompanied by the creation of a new PNT Unit in DSIT.

I am particularly grateful to the individual problem owners (in both Government and Industry) and the world-class group of researchers who contributed so positively and generously to our discussions. I have no doubt that their insights, summarised in these pages, will clarify – even transform – readers' understanding of the issues, and pave the way for building greater resilience in our Critical National Infrastructure.

Dr. Tristram Riley-Smith
Associate Fellow,
Centre for Science & Policy,
University of Cambridge,
10 Trumpington Street, Cambridge CB2 1QA.

28 March 2024.

1 Introduction

The Resilience and Security Institute at Cranfield University has teamed up with the Centre for Science and Policy (CSaP) at the University of Cambridge to host a roundtable on Building Resilience in the UK's electromagnetic environment (EME). The work was supported by the Academic Resilience & Security Community (now rebranded as NSEC – the Network for Security Excellence and Collaboration) and the 2-day event was sponsored by Leonardo UK. The goal of the roundtable was to encourage the exchange of knowledge, insights and ideas among the participants coming from problem owners, policymakers, industry representatives, and researchers. A timetable of the event is provided in Appendix A: Roundtable Agenda. The workshop should further support the role of NSEC and act as a bridge between the work of government and academia.

Modern systems, including critical national infrastructure (CNI), heavily rely on the EME and are interdependent. Changes in the EME, both due to natural causes (e.g. space weather) or malicious intent (e.g. jamming), can have damaging effects and could have huge implications on all sectors. Therefore, it is vital to build resilience in the UK's EME. The concept of resilience describes the ability to anticipate, prepare, respond and learn. The roundtable aimed at identifying risks, describing vulnerabilities, designing mitigation strategies and developing recovery plans.

The round table discussion included experts from government, industry and academia to discuss the embedded challenges of the EME. Two breakout sessions were part of the roundtable and delegates were split into five groups, each addressing questions on Threats, Vulnerabilities, Risk Management, Mitigation Strategies, and Recovery, respectively (see Appendix B: List of Questions for Breakout Groups). This report combines the outputs of those two breakout sessions and divides them into identified threats and vulnerabilities (Chapter 2) and recommended solutions (Chapter 3). The names of all attendees are listed in Chapter 4.

2 Threats and Vulnerabilities

2.1 Natural

- **Space Weather**
  - The Carrington Event in September 1859 remains the largest geomagnetic storm to hit the Earth; it caused telegraph systems across North America and Europe to fail;
  - We have not experienced a "Carrington" class event in a long time; smaller Space Weather events do, increasingly, present issues for the CNI and a Carrington-scale event (or worse) is expected to happen in the future;
  - Severe space weather is captured as a risk on the UK's *National Risk Register* (2023); but exact space weather is difficult to predict and there is no full assessment of what a similar event to Carrington would mean to the current EME with more reliance on technology[1];
  - However, there are reasons to be concerned given the importance of EME to our CNI:
    - Energy Infrastructure & Power Supply: a 2022 study[2] conducted for the New Zealand Government suggests that between 13% and 35% of transformers are at risk from damaging levels of induced currents;
      - Given a lead time of many months to replace a single transformer, a future Carrington Event could severely impact the National Grid;
      - It is unclear what the cascading effects on other sectors (e.g. telecommunications and transport networks) would be.

[1] A handful of economic impact studies have been conducted but information is difficult to pin down and there are gaps given the development of contemporary technology. (See recommendation R09)
[2] Mac Manus DH, Rodger CJ, Dalzell M, et al. Geomagnetically Induced Current Modeling in New Zealand: Extreme Storm Analysis Using Multiple Disturbance Scenarios and Industry Provided Hazard Magnitudes. Sp Weather. 2022;20

        - Communication Systems:
            - There would be significant disruption and potential loss of satellite communication
                - Severe space weather would introduce significant additional atmospheric drag on satellites but with an uncertain impact on satellite infrastructure
            - Some level of both space and ground-based signal disruption is expected, including to Global Navigation Satellite Systems (GNSS)
            - Geomagnetic storm disruption can be driven over multiple days, with an extended recovery phase: long-term impacts would arise as cumulative damage accelerated ageing and brought forward out-of-service dates.
            - Impact on the mobile system for masts facing the sun
    - Not just extreme events but increasingly also day-to-day events present issues for CNI.

- **Geomagnetic Field Reversal**
    - The Earth's geomagnetic field periodically alternates (swapping positions of magnetic north and south). This is a slow and rare process[3] but it will happen at some point and poses a significant long-term threat
        - Navigation will move from magnetic north to true north coordinates
        - Multiple magnetic poles could be present during the transition to a full magnetic field reversal

[3] On average, it happens every 450,000 years. The last was 780,000 years ago

2.2 Man-Made

- **Jamming**
  - Becomes more and more democratised as access to devices and technology is readily available
  - The threat is deniable as effects can be turned off immediately
  - Jamming is also used in Electronic Warfare (see below)
  - Examples of technologies that can be easily jammed include:
    - Signals from GNSS
    - Mobile masts
    - Automatic Dependent Surveillance-Broadcast
    - Wifi
  - Issues also derive from the use of small jammers e.g. on cars
    - Enablers for serious criminality e.g. interfering trackers on stolen vehicles to hide them
- **Electronic Warfare (EW)**
  - Conventional Electromagnetic Pulse (EMP)
    - Effects depend on the intensity of the pulse
    - Current trend on directed energy weapons (DEW)
      - E.g. Laser and radio frequency (RF)
    - Several countries are running programs on DEW
      - Currently few, very exquisite systems with the capability to severely impact CNI
  - Nuclear EMP
    - Short-lived, high-transit pulse could have a significant impact on CNI

2.3 Systemic

- **Systems become increasingly interconnected and there is uncertainty over their product capability**
  - The result is a lack of understanding of how resilient the technology is to electromagnetic interference
    - Organisations do not have resilience to interference as a high priority and therefore do not include the requirement in their procurement

specification to minimise costs. The overall lack of investment is a major concern.

- Most companies make rational economic decisions and do not buy equipment for a one-in-a-hundred-year event

- Impact on one part of the system could lead to cascading effects and cause undeterminable impacts on other parts of the system
  - There is a general lack of understanding of how systems work and their interdependencies
    - No model or simulations are currently available
    - Limited understanding makes targeted investment and prioritisation challenging
    - Systems and mitigations are still quite siloed
    - UK has a National Risk Register (NRR) but local risk may vary
    - Identification of risks has not always moved towards mitigation and preparedness
  - The threat is amplified by commercial organisations not sharing data
    - Lack of access to commercially sensitive data (e.g. aviation and satellites) results in manufacturers not willing to share information on their products, particularly the vulnerabilities of their systems
  - Lack of data set comparison
    - Assessment of what and how systems are reacting to low-level interference challenging
- Dependency on GNSS and its timing capability to synchronize networks
  - Telecommunications networks have atomic holdover clocks at the centre of the network that provide a level of redundancy
  - Important for example for positioning in the aviation and maritime industry
  - GNSS is highly vulnerable to low-level interference
  - Resilience and backup to CNI systems are not formally addressed
    - There are developments for the introduction of a network of atomic clocks in the National Timing Centre

    - Recovery after disruption
        - Will depend on the cause, impact and duration of disruption
        - Concerns over governance structure and communication strategy to provide a robust CNI
        - Limited understanding of how we would bring systems back up
- **Loose legal framework and enforcing mechanism**
    - There is a lack of legislation for product compliance
    - Requirements for detection and prosecution of interference and protection of frequency bands in EME
- **Skills gap may lead to a lack of expertise to maintain and develop existing system**
    - The number of RF engineers and designers is decreasing while the number of software engineers is increasing
    - The shortage of RF skills is recognised nationally
- **Lack of community preparedness**
    - Society is unprepared for handling severe disruption to CNI
        - Experience from Covid has demonstrated panic buying behaviour
- **Age of acceleration**
    - The rate of change in technology is changing and advancement in technology also makes systems more vulnerable
    - The influence of Artificial Intelligence will provide challenges but also opportunities
- **Lack of stockpiles and backup systems for disruptions**
    - Drive for more efficiency and the absence of experiencing severe events in a long time has led to a reduction in stocks and backup systems
    - Global geopolitical conflicts have further diminished the supply
        - UK has donated transformers to Ukraine
        - Re-supply will take time due to global supply chain disruption and concerns over available engineers to replace parts

3 Solutions and Recommended Actions

The overall recommendation was to foster collaboration between government, industry and academia and promote research in the area of EME resilience. Furthermore, it was reiterated that it is important to move away from an "*if it happens*" towards "*when it happens*" thinking and approach. The following 20 recommendations (R) were thematically grouped into four categories.

3.1 Promote a "Resilience by Design" approach

R01: Create a resilience culture for engineers and designers

- Work towards a similar culture to Security-by-Design
- For example, in the US the Institute of Electrical and Electronics Engineers have a working group (P1952) determining requirements for resilience in order to test and verify CNI components
- Royal Academy of Engineering (RAEng) has provided a good starting point with its 2013 report[4] which could potentially lead to further work

R02: Drive investment in resilience

- Investments are needed in alternative PNT
- Alternative PNT should not be space-based to provide redundancy
    - The Department for Science, Innovation and Technology (National PNT Office) and the National Physical Laboratory (own the National Timing Centre programme) could take a lead on that topic

R03: Strengthen regulation through legislation

- The government could consider mandating standards to provide resilience
    - E.g. Surviving a one-in-a-hundred-year event
- Specify new and enforce current standards (e.g. similar to electromagnetic compatibility directive)

[4] Royal Academy of Engineering. Extreme Space Weather: Impacts on Engineered Systems and Infrastructures. London, UK; 2013. http://www.raeng.org.uk/news/publications/list/reports/Space_Weather_Full_Report_Final.PDF

- Establish procurement guidelines and a catalogue of recommended products that fulfil requirements
- Provide incentives for research on required technology leading to more resilient products and provide incentives to encourage radiation environmental system testing

R04: Invite the insurance sector to incentivise resilient electromagnetic design

- Conduct a cost-benefit analysis to justify investment
- Investments in resilience could be rewarded through lower premiums

R05: Invite National Grid to share knowledge of its work on managing risks arising from electromagnetic threats

  - Support National Grid's efforts to invest in resilience through peer review, for example via the RAEng or Space Environment Impact Expert Group
  - Encourage National Grid Electricity System Operator to apply learnings from other contemporary resilience studies (e.g. New Zealand study referenced on p 3) for the best possible outcome from their own assessment studies
  - Explore opportunities for more resilient and localised power networks (e.g. relying on solar and wind if National Grid is damaged in an event)

R06: Stress test existing CNI

- Test failure of specific sectors of the CNI (following example of the Financial Conduct Authority stress testing banks)
- Test the failure of individual sub-systems and evaluate the impact on the wider network resilience due to the interconnected nature of CNI

R07: Review the feasibility of a kitemark for resilience product compliance

- The goal is to influence consumer behaviour by providing more information on the electromagnetic resilience of electronic products
  - Conduct market research to see if the potential is there and how the idea can be operationalized

- Strengthen enforcement through the legal system (e.g. penalising the use of unsecured systems by CNI operators)

- British Standards Institution could take the lead

R08: Review strategy for power resilience of CNI systems

- Examples include:
  - Stockpile spare transformers to quickly replace damaged systems
  - Standby generators to support the grid during the repairs
  - Back-up system for (tele-)communication networks
    - eLoran service for timing and emergency services
    - Atomic clocks as backup systems
  - Use of different frequencies to introduce diversity for events that may impact the communication system
    - Reliance on diverse bands for improving redundancy

R09: Review learnings from past studies

- RAEng has made many relevant recommendations: have they been implemented?
  - See the RAEng report[5] from 2013 on extreme space weather and impacts on engineered systems and infrastructure
- Analyse report issued by Lloyds[6]
- Refer to the technical report issued by UK Research and Innovation[7]

[5] Royal Academy of Engineering. Extreme Space Weather: Impacts on Engineered Systems and Infrastructures. London, UK; 2013. http://www.raeng.org.uk/news/publications/list/reports/Space_Weather_Full_Report_Final.PDF

[6] Hapgood M, Thomson A. Space Weather - Its impact on Earth and implications for business. *Lloyd's 360° Risk Insight*. 2010. https://assets.lloyds.com/media/ec9c7308-7420-4f1a-83c3-9653b1f00a4c/7311_Lloyds_360_Space Weather_03.pdf.

[7] Hapgood M, Angling M, Attrill G, et al. Summary of space weather worst-case environments (3rd revised edition). UK Res Innov. 2022;RAL-TR-202. https://epubs.stfc.ac.uk/work/51273983.

R10: Seek the active engagement of Learned Societies and Professional Bodies in addressing the challenges

- There are many organisations well-placed to help. E.g.:
  - RAEng
  - The Royal Society
  - Register for Security Engineering Specialists
  - Institute of Telecoms Professionals
  - Institute of Engineering and Technology
  - Institute of Physics
  - Institute of Civil Engineers
  - Royal Institute of Navigation

R11: Consider the following examples for more resilient product design

- Faraday cages and electromagnetic compatibility gasket to protect sensitive equipment and sites
- A specific example was presented at the workshop:
  - The low-cost anti-jamming system produced by Roke Manor
    - Consists of a four-element antenna array that forms an omnidirectional radiation pattern until noise is detected and removes up to three sources of interference
    - Installed in communication systems used in Afghanistan to solve electromagnetic noise issues.

3.2 Promote better risk management

R12: Develop a secure platform to allow sharing of commercially sensitive data

- Review whether or not *Resilience Direct* (https://www.resilience.gov.uk/) could be used to facilitate data sharing
  - With the use of privacy-preserving mechanisms and anonymisation?
- Review work of Local Resilience Forums (LRF) and adopt best practices
- Consider mandating that a minimum amount of data is shared

R13: Apply system thinking to outline the complexity of the system of systems and how disruptions cascade

- Drive consistent risk philosophy
  - Encourage businesses to think more clearly about their approaches to risk (given evidence that Boards are disinclined to invest in rare – e.g. one-in-a-hundred-year event– risks regardless of scale of impact);
    - Mandating will be required to drive work forward
- Draft multiple disruption scenarios with different scales and aspects
  - Understand 2nd order effects and map out dependencies
- Capture the interaction of different systems and different technologies

R14: Set up platforms to develop and share a National Risk Model

- Potential existing platforms
  - Explore Data & Analytics Facility for National Infrastructure (DAFNI) for further work
    - DAFNI hosts a computing platform for models and data from industry, government and academics on national infrastructure for planners and decision-makers
  - National Computing Centre could also be used
- Ensure access to the digital model
  - The model will include sensitive information about UK CNI and therefore security of information needs to be ensured

R15: Build a national plan for how to respond to a severe disruption of the EME

- Rank which systems need to be given priority for investment and recovery
- Focus on both day-to-day disruptions and large-scale events
- Use it to develop mitigation strategies and how to recover from a crisis

3.3 Address knowledge and skills gap

R16: Develop engineering skills to recover infrastructure in the event of disruption

- E.g. Launch *1000 Engineers* initiative to create national capacity to respond to electromagnetic crisis
  - With systems knowledge/specialism and transferable skills
  - In addition to technical expertise, engineers also know how to work together with people from different backgrounds, skills and discipline areas
  - Designing an effective reward and retention scheme to underpin this initiative
- Government-sponsored education schemes

R17: Amend existing training to encompass electromagnetic resilience

- Engage with potential partners to develop additional programmes
  - the UK Resilience Academy (previously Emergency Planning College) could have an important part to play here

3.4 Raise awareness and increase preparedness

R18: Run an information campaign to raise public awareness and provide the public with instruction on how to prepare

- Engage with behavioural scientists and communication experts

R19: Develop governance structure and communication strategy for handling disruptions in EME

- How do we communicate with the public and businesses after a major disruption when certain systems (e.g. telecommunication) are not available?
  - E.g. All cars in the US need to have an AM radio
- Create Office for Catastrophe Resilience
  - Consider having a new Chief Scientific Adviser dedicated to this office
  - Representatives are at the right level of seniority appointed position in government
  - Independent body from the government

    - Long-lasting positions which are not tied to electoral cycles
    - Different vertical and horizontal interests are represented
    - The office ensures individual sets of preparedness do not conflict (e.g. service providers are not using the same backup systems or capabilities)
- Strengthen the role of LRFs
    - For achieving a higher level of preparedness and for recovery from events

R20: Run National Exercise

- Large-scale exercise with multiple impacts to test preparedness for and recovery from severe disruption
    - Will most likely involve loss of GNSS and other critical systems
    - Outputs can be used to identify interdependencies of the system
- Extensive preparation required
    - Previous exercises took 7 months of planning for a 2-day exercise
- Attendees were made aware that preparations for such an exercise are currently taking place
    - No immediate support was currently required
- Equivalent to a “National Fire Alarm”

4 Attendees

- **Dr Anas Al Rawi** (Principal Technology Advisor, Networks & Communications Group, Ofcom)
- **Prof. Gemma Attrill** (Lead Scientist, Space Systems Programme & Chief Scientist, Space Weather at Dstl)
- **Dr Alessio Balleri** (Professor of Radar Systems, Cranfield University)
- **Mark Beach** (Professor of Radio Systems Engineering, University of Bristol)
- **Peter Bristow** (Policy Lead, Telecoms Security & Resilience, DSIT)
- **Paul Curtis** (Design Authority for Cyber Electro Magnetic Activities, Thales UK)
- **Dr Jurgen Doornik** (James Martin Fellow, Institute for New Economic Thinking, University of Oxford)
- **Dr Stuart Eves** (Consultant in Space Industry, SJE Space Ltd)
- **Prof. Joanna Faure Walker** (Professor of Earthquake Geology & Disaster Risk Reduction, UCL)
- **Jessie Hamill-Stewart** (Cyber Security PhD candidate at Universities of Bath & Bristol)
- **Dr Will Handley** (Royal Society University Research Fellow & Turing Fellow, University of Cambridge)
- **Dr Simon Harwood** (Capability and Innovation Director, Leonardo UK)
- **Mark Henry** (Director of Network & Spectrum Strategy, BT)
- **Dr Duncan Hodges** (Strategy & Technology Group, Leonardo UK)
- **Prof. Richard Horne FRS** (Head of Space Weather, British Antarctic Survey)
- **Dr James Kelly** (Senior Lecturer, Reconfigurable Microwave Antennas, Queen Mary University London)
- **Nigel Lyons** (Lead for Industry & Policing Liaison Police, Office of the Police Chief Scientific Adviser)
- **Simon Machin** (Space Weather Lead, Met Office)
- **Dr Trevor Maynard** (Exec Director of Systemic Risk, Cambridge Centre for Risk Studies University of Cambridge)
- **Edward McBryde-Wilding** (Police Adviser, Home Office Science & Technology Commissioning Hub)
- **Prof. Cathryn Mitchell** (Professor of Electronic & Electronic Engineering, University of Bath)
- **Iain O'Brien** (Head of Spectrum Compliance, Ofcom)
- **John I.R. Owen** (Founder, Border Consulting)
- **Dr Gianluca Pescaroli** (Associate Professor, Operational Continuity & Organisational Resilience, UCL)
- **Calum Ronald** (Senior Risk Consultant, Pool Re)
- **Prof. Keith Ryden** (Professor of Space Engineering, University of Surrey)

- **Prof. Simon Saunders** FRAEng (Advisor & Researcher, Communication Systems Technology, DSIT & KCL)
- **Prof. Yeshpal Singh** (Professor of Quantum Science & Innovation, University of Birmingham)
- **Dr Annette Southgate** (Director of Security, Cranfield University)
- **Dr Neil Stansfield** (Head of Strategy and Digital Sector, National Physical Lab)
- **Hayley Trezel** (Head of CNI & Critical Supply Chains, Resilience Directorate, Cabinet Office)
- **Andy Wells** (Head of Policy, Civil Aviation Authority).

Lightning Talk Presenter (online)

- **Prof. Alexandra Brintrup** (Professor in Digital Manufacturing, University of Cambridge)*
- **Steve Hancock** (Lead Scientist, Position, Navigation & Time, Ordnance Survey Ordnance Survey)

Facilitators

- **Prof. David Denyer** (Professor of Leadership and Organisational Change, Cranfield University)
- **James Hill** (Defence & Security Programme Manager, Cranfield University)
- **Nick Lindley** (Campaign Director for Defence & Security, Cranfield University)
- **Dr Tristram Riley-Smith** (Associate Fellow, Centre for Science & Policy, University of Cambridge)
- **Mike Sutliff** (Senior Lecturer in Innovation and Change, Cranfield University)

Report writer:

- **Dr Fabian Steinmann** (Lecturer in Organisational Resilience & Change, Cranfield University)

Appendices

Appendix A: Roundtable Agenda

Monday 5 February

1200 Registration

1230 Lunch

1345 Plenary (LR17): *Opening Remarks*
- Launch: Tristram Riley-Smith
- Welcome to Cranfield: Prof. David Denyer
- Intro to Academic RISC: Annette Southgate
- The Significance of the Challenge: Simon Harwood
- Open Forum: Problem-Owners invited to surface key concerns.

1430 Breakout Groups*: *Unpacking the Issues and Challenges*
- LR17: Groups 1, 2 & 3
- LR18: Groups 4 & 5.

1600 Tea Break

1615 Plenary (LR17) *Lightning Talk: Professor Alexandra Brintrup, IfM*

1645 Plenary (LR17): *Feedback from Breakout Groups*

1800 Close: delegates to find bedrooms etc

1830 Drinks Reception

1915 Dinner

Tuesday 6 February

0900 Plenary (LR17) *Lightning Talk: Stephen Hancock, Ordnance Survey*

0930 Breakout Groups* - *Developing Solutions and Recommended Actions*
- LR17: Groups 1, 2 & 3
- LR18: Groups 4 & 5.

1100 Coffee Break

1115 Plenary (LR17): *Feedback from Breakout Groups*

1245 Plenary (LR17): *Wash-Up/Close-Down*

1300 Lunch

1400 Delegates depart.

Appendix B: List of Questions for Breakout Groups

Group 1: The Threat?

- What is the reality about the threat posed to 21st Century systems through disruption to the electromagnetic (EM) environment by:
  - Space Weather (SW) e.g. Radiation or Geomagnetic Storms
  - An EM Pulse device
  - Use of heavy-duty jamming or spoofing
  - Propagation effects of a tactical nuclear bomb exploded 1,000s of miles away (eg Ukraine)?
- Are there other threats and how will these change over the next 5-20 years?
  - Can we assess the unintentional damage caused by spectrum-sharing & deregulation?
  - How can we ensure the integrity of UK infrastructure given as international threats evolve?
  - How will pace-of-change in emerging technologies (eg AI) help bad actors deliver EM disruption?
- How can resolve attribution, to get clarity on any threat at speed?
  - Are networks of specialists in place to address challenges if the EM environment is disrupted?
  - What data and/or tools do different sectors & operators require to identify the source of a problem?
- How likely are these threats to occur?

Group 2: Vulnerabilities?

- How susceptible are our systems/networks to these threats?
  - How well do we understand issues within our Critical National Infrastructure (CNI) regarding interference with the EM spectrum, including interdependencies and the consequences of knock-on or cascading effects?
  - How can we monitor, measure & analyse this? Are tools & technical expertise available to make an assessment?
  - Do we have the right industrial standards and use them effectively: what protection is deployed where?
  - How would a major space weather event affect not just GNSS satellites in MEO but the whole PNT system of systems including LEO, eLORAN, and even terrestrial systems as well?
  - are CNI microchip control systems resilient against a 1-in-50-year or 1-in-100-year SW event?
  - How vulnerable are the internet, terrestrial telecoms, subsea cables, fibre optics to EM disruption?
- Will the EM environment change over next 5-20 years, increasing vulnerabilities?
  - E.g. the growth of Smart Cities, Internet of Things, Autonomous Vehicles, 6G

Group 3: So What & Risk Management?

- Do we have the tools and techniques to model the impact on national wellbeing?
  - Is there any value in discriminating between effects of different scenarios or is it more sensible to build resilience based on a reasonable worst-case scenario?
  - Is the "reasonable worst-case scenario" presented in the National Risk Register credible & sufficient?
  - How can we assess the scale of disruption after loss of GNSS systems to: supply chains (esp 'last mile delivery'), Emergency Services, Telecoms Systems, Power Networks, Aviation and Financial Services?
    - do we understand the range of interdependencies between critical systems and enabling technologies?
    - how can we analyse cascading effects (e.g. if the timing controls of electricity sub-stations are knocked out)?
    - how can we assess impacts on day-to-day life (e.g. transport hubs, ability to communicate, behaviours and mental health)?
    - Can we calculate the financial impact of deploying an EMP or jamming device in the City of London (or other targets in the UK where a successful EMP or jamming attack would impose substantial financial costs)?

- Knowledge and Communication
  - do we have a shared understanding of the risks? Are risks and risk management solutions being communicated effectively to all who need to know (including CNI and Lead Government Departments)?
  - What is being done to coordinate or promote effective mitigation / resilience with either individual companies or sector-wide? Is there effective training and/or exercising in place?
  - what is the quantity/quality of information collected during an incident; how can this be improved?

- What more needs to be done to make this a 'whole of society' endeavour?
  - who needs to contribute and how can they be empowered? What should we expect from businesses (e.g. sharing vulnerability data), the local tier, voluntary organisations, community groups, and the public?
  - what is the role of Government/legislation here? Are the right incentives/levers in place to mitigate effectively?

- have we got effective Risk/Crisis Management processes, structures and standards?
  - who needs to be involved: CNI operators, regulators, LDGs, supply chain companies, service-providers, etc?
  - which overseas partnerships could help (taking account of geopolitical, scientific, and technological factors)?
  - Do we need better standards (inc for emerging technologies such as Quantum & AI?

Group 4: Mitigation?

- What does a good mitigation strategy look like?
  - is there evidence that such strategies are up and running?
  - Should this span the whole risk cycle, including risk prevention and building resilient systems?
  - What investment is needed to improve resilience to EM phenomena, and where do costs accrue?
  - Are there current capabilities (technology, skills, partnerships) which are not being exploited at all (or not sufficiently well)?
  - Is it important to measure the effectiveness of mitigations; if so, how?
- Can research help address these specific challenges:
  - what alternative space-based PNT technical concepts could be considered for the competitive, congested and contested GNSS RF environment that could support Low-Earth Orbit missions?
  - how can we undertake *system-of-systems* analysis across the wider PNT community, to help identify and isolate what is required from the space-based service?
  - timing is critical for telecoms: what are the best range of solutions to deliver greater resilience?
- what Emerging Technologies could improve resilience economically over 5-20 years?
  - How will AI change our ability to build resilience of our EM environment?

Group 5: Recovery?

- Given that absolute resilience and mitigation is not likely …
  - Do we understand what recovery looks like and should we consider a range of recovery scenarios based on unmitigated risks, partially mitigated risks and optimally mitigated risks?
    - Consider the impact of operating with degraded technologies for a period of time;
    - Consider damage incurred and repair (global supply chains) and time to recover/repair;
    - Consider international landscape and geopolitical prioritisation/leverage;
    - Consider possible new latent vulnerabilities;
    - Consider economic and social implications and challenges.
- What does a good recovery strategy look like?
  - is there evidence that such strategies are in place?
  - Is investment needed to assist the operators of critical infrastructure and systems to develop recovery plans?
  - Are there current capabilities that could inform recovery (technology, skills, partnerships) which are not being exploited at all (or not sufficiently well)?
  - Do we need to invest in sovereign or international partnership capabilities to ensure rapid recovery can take place?