Royal Academy of Engineering

Critical capabilities:

strengthening UK resilience

"With the Integrated Review, we are placing greater emphasis on resilience, building resilience at home and overseas, and our first goal is a commitment to strengthen our national resilience. The Royal Academy of Engineering's Critical Capabilities report proposes an alternative way of thinking about what comprises our national capability, adopting systems approaches to help build whole society resilience and leverage the UK's strengths"

Professor Dame Angela McLean DBE FRS
Chief Scientific Adviser for the Ministry of Defence

"Science and engineering have played a crucial role through the COVID-19 emergency, helping find viable pathways out of this pandemic. We must remind ourselves that this was possible because of decades of sustained investment in people, research and facilities. The Critical Capabilities approach identifies the full range of capabilities, investments and connections needed to be well prepared for when the next emergency hits, including the UK's outstanding science, research and innovation capabilities"

Sir Adrian Smith PRS
President of the Royal Society

Foreword

2020 brought unprecedented disruption and restrictions to our daily lives, and intense strain on healthcare systems, businesses and economies across the world. We experienced challenges and tragedy as the pandemic unfolded, but also hope as a path out the crisis emerged. Many saw for the first time the breadth of capabilities needed to respond to an emergency of this scale – from key workers, healthcare practitioners and volunteers to the role of rapid innovation in delivering new healthcare solutions and social distancing technology, how agile manufacturing supply chains can pivot to deliver critical equipment, and the remarkable development of safe effective vaccines from inception to injection in less than a year.

Even as the crisis was evolving, a fundamental question was already emerging: how can the UK be more resilient to address the emergencies of the future? And in the engineering community, how can we help?

As engineers, we think of resilience by examining the systems in front of us, understanding interconnections, dependencies and vulnerabilities to identify those safety critical roles or layers of mitigation preventing unacceptable failure. So, in late 2020 we took this engineering mindset and characteristic systems approach and applied it to the challenge of strengthening our resilience to the emergencies of the future, in the knowledge that emergencies will always arise and that each will be different. Rather than base this study on the still active COVID response, we based our evidence on UK national and local responses to emergencies of the past and built an understanding of the interconnected and interdependent system of capabilities for UK resilience.

We have termed our findings critical capabilities: the people, resources and infrastructure we draw on in a crisis to respond, quickly and effectively. We found that the ability to respond rapidly and well – to know who to contact, and how to act – hinged in large part on how well the authorities had anticipated which parts of this wider system would be relevant to the emergency in question, and how well networked they were in advance. We found examples of crucial connections that were overlooked, and weaknesses that not been successfully addressed years later.

Each emergency defines the relevant system boundary, the capabilities most needed to respond well this time around. For most emergencies of scale, this will go far beyond the well-networked elements of the public sector and blue light services which are geared to respond to emergencies, and will include the private sector, international relationships, research and innovation, national assets such as the Met Office, and the interfaces between them. Understanding where that boundary lies and holding the ability to access the relevant capabilities at speed is crucial to an effective response. We offer new thinking both on specific practices to enable greater preparedness, but also on how to embed this overarching ability to understand the system and prepare it for future shocks.

With the recent publication of the Integrated Review, now is the time to think ahead, strategically and inclusively. This is an investment for the UK, to build upon our capabilities, strengthen our resilience to whatever uncertain emergency lies ahead, and compete globally as a science and innovation superpower.

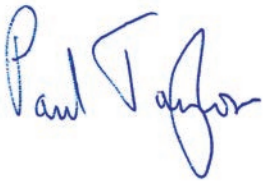
Professor Sir Jim McDonald FREng FRSE
President of the Royal Academy of Engineering

Foreword

The COVID-19 pandemic is a stark reminder of the importance of resilience and preparedness. With this in mind, the Working Group came together to see how the UK could be more resilient to future emergencies, in all their possible variety and uncertainty. Critical capabilities proposes an engineering approach to help build whole-society resilience, and to leverage the breadth of UK capabilities, across the public and private sector.

Lessons from the past sometimes still need learning for future preparedness, and our workshops effectively re-lived historical emergency responses with people involved at the time and asked whether we are better prepared now. This process, and the open, honest discussions it enabled, were hugely valuable to understand the different components of the response, how they came together, what went well and what could be better. What really struck me was the importance of those relationships and networks that had been built and exercised in 'peace' time and were ready to activate and manage the uncertainty of an emergency unfolding. My experience working in both the public and private sector in defence and security has shown me time and again how crucial practice and a shared understanding of each other's capabilities and vulnerabilities really is.

It was a pleasure chairing this project for the Royal Academy of Engineering, and I extend my thanks to the Working Group and the Academy team for their invaluable contributions to this work.



Paul Taylor FREng
Chair of the Critical Capabilities Working Group

Contents

Executive Summary

The COVID-19 pandemic has already had a profound impact on health and wellbeing, daily life, and the economy around the world. This emergency is ongoing and its full lessons will take time to learn. But it is a stark reminder that emergencies do happen, and how well we respond to them is highly dependent on the capabilities that we have in place.

One question emerging from this emergency is **how to build a more resilient future?**

The Integrated Review calls for a 'whole-of-society' approach to resilience, so that individuals, businesses and organisations all play a part in building resilience across the UK. In this report, we apply an **engineering mindset**, and set out how a systems view which focuses on broad "**critical capabilities**" needed for an emergency response can enhance the current approach to UK planning, preparedness and can strengthen UK resilience. This includes three practical recommendations on page 7 aimed at government working in partnership with engineers to support the development of the national resilience strategy work which is already underway.

How an engineering perspective can help

Engineers are trained to make things work better. They examine complex systems, assess risk and its potential propagation, and identify how that system can continue functioning safely even under severe stress. Applying this engineering mindset, we see emergency response and planning as a series of **interdependent and interconnected systems of capabilities** designed to improve the UK's ability to respond to emergencies and threats, one which engineering can help to understand and optimise using skills such as problem definition, creative problem-solving, and systems thinking.

An effective national response to an emergency or crisis is one that can rapidly call on the right capabilities to deliver the most effective response at the required pace. This report describes this in terms of 'critical capabilities': the UK's system of people, infrastructure and assets that build short- and long-term resilience within an interconnected world. This project aims to explore how a wider, systems-based view of the broad capabilities needed for an emergency response can enhance the current approach to planning, preparedness and build resilience.

Resilience is the ability to anticipate, resist, absorb, recover, and adapt to shocks and stresses in the system with agility, to enable continuity of delivery of critical needs such as safety, food, energy, and healthcare. This report sets out an engineering perspective on strengthening resilience to emergencies by focusing on the actions that can be taken to identify and build critical capabilities in anticipation of an emergency. It makes recommendations for government to embed this approach into UK emergency planning and preparedness to facilitate a rapid and effective response. It draws upon lessons from four past emergencies (listed in Figure 1) that are presented as individual case studies, and synthesises the evidence and insights from desk-based research, interviews and workshops with individuals and experts involved in the emergency responses at the time. The four case studies were chosen to reflect a range of emergency characteristics (physical/digital disruption, central/local coordination, and national/international impact).

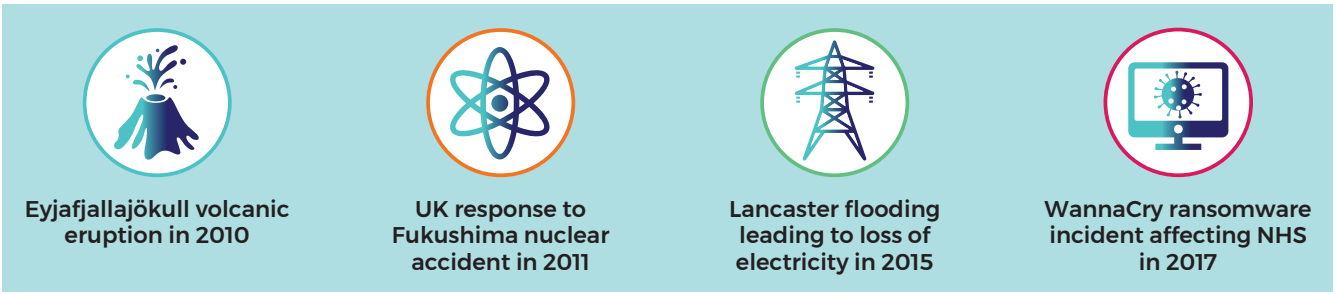


Figure 1: Critical capabilities case studies

Keeping pace in an age of change

We live in an age of ever faster social and technological change, and with greater sophistication comes both the need to develop new capabilities and address new vulnerabilities. To keep pace, we must learn the lessons of each emergency we face, draw on national and international insights and horizon scanning to anticipate how things may be different next time. Combining lessons from past events, near misses and strategic foresight can better inform investment in wider resilience and implement improvements to our preparedness for future challenges.

The critical capabilities approach

Critical capabilities are divided into six intrinsically interdependent capability groups – **research and innovation; national assets; industrial capability; skills and labour; and resources – with networks and coordination capabilities acting as the sixth bridging capability that brings these together to understand the issue and accelerate solutions** illustrated in Figure 2.

This report focused on examining why networks and coordination capabilities are **necessary in an emergency response and why they should be routinely considered in preparedness and planning to improve resilience**. By focusing on networks and coordination, this report explores how all the underpinning capabilities come together, to identify the challenges and enablers that can hinder or support an effective emergency response. **The case studies were used to test and build a broad consensus of the critical capability groups and help to identify cross-cutting lessons; these 'practices for preparedness'** are described further in the next section.

Practices for preparedness

By investigating past emergencies through the **cross-cutting lens of networks and coordination capability**, the report has identified themes and lessons that could be adopted by public, private and third sector organisations to improve the ability to respond to the next emergency, whatever it entails. While framed as government processes for preparedness, these '**practices for preparedness**' can be applied more widely and help organisations build and strengthen capabilities, improving their resilience for future emergencies. While many of these practices will already be commonplace, recovery from the current emergency provides an opportunity to reflect and assess against these six practices with more detailed considerations in the report.

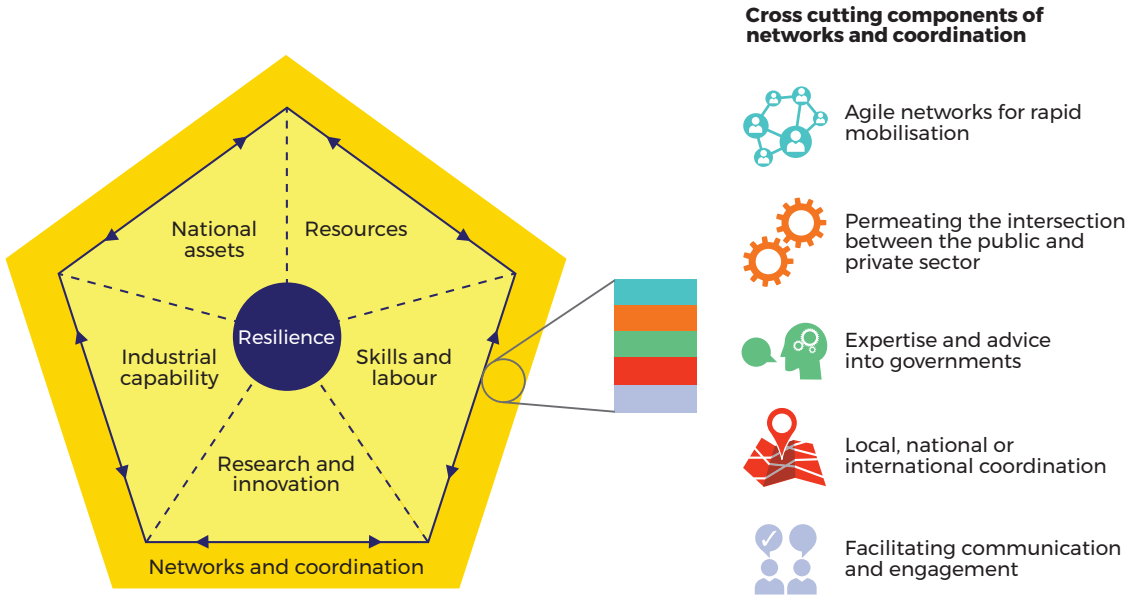


Figure 2: Critical capabilities

- **Understanding**: mapping of national, local and organisational capabilities, what they can provide and identification of gaps.
- **Relationships**: building and maintaining a network of networks of local, national and international relationships.
- **Resilience by design**: improving preparedness and response of organisations, processes, infrastructure, and facilities.
- **Responsibility**: ensuring clear ownership of resilience at every level.
- **Exercise**: practising responses to build relationships, increase awareness of existing capabilities and better prepare for a range of emergency situations.
- **Agility**: keeping pace with increasing digital interconnectedness and evolving threats and hazards.

We are calling upon leaders in the public, private and third sector to reflect upon the extent to which these practices for preparedness are incorporated in their business continuity plans or emergency response planning and act upon them. All organisations need to consider where their interdependencies lie within the wider system, how vulnerabilities can be reduced and resilience strengthened.

We are also calling upon individuals and organisations to raise questions and test policies and decisions against these practices for preparedness to ensure resilience isn't considered as an after-thought by decision-makers and responsibility for resilience is clear across organisations.

Recommendations for government

Emergency response at scale requires effective engagement and coordination of capabilities across the public, private and third sector. This can be challenging to incorporate into all current emergency preparedness processes. The case studies **highlighted instances where the systems' boundary didn't go wide enough to consider all of the relevant stakeholders or the interconnections within weren't strong enough or leveraged effectively at the onset of the emergency**. Applying a wider systems-based view and building a consideration of critical capabilities would guide and shape the implementation of the practices for preparedness with:

- a structured identification of the breadth of critical capabilities across the public, private and third sector and the flexible role they play that can enable emergency response to both mitigate risks and seize opportunities
- an understanding of the interdependencies that exist across risks and response to mitigate concurrent and compound risks with potential for cascade failure, where multiple elements happening at one time trigger an emergency or an initial failure initiates a cascade of failures across an interconnected system
- the determination of the critical networks and coordination capability for emergency response to ensure they can be involved and strengthened in planning
- wider engagement with and from the private sector to leverage their capabilities, such as agile manufacturing capability, skills and expertise, and international connections for faster and more effective responses.

This report calls for practical action to build systems thinking and consideration of capabilities deeply into our approach to preparedness enabling adaptability and agility with the implementation of the Integrated Review including the development of the national resilience strategy 2021. Whatever practices and procedures are in place, they risk missing the mark if this is not in place. While this will require upfront investment to strengthen existing capabilities and remedy gaps, immediate and long-term benefits can be delivered through improved emergency response and national resilience. Investment in our existing capabilities goes beyond just provision of insurance for future emergencies, it can deliver wider benefit to the country and society.

The Integrated Review calls for a whole-of-society approach to resilience, so that individuals, businesses, and organisations all play a part in building resilience across the UK. To support this ambition, we are calling on government to partner with the engineering profession and others:

1. **Government should embed a systems approach in emergency planning and preparedness, looking across the public and private sector stakeholders**.
   - Training in systems approaches should be provided to resilience teams across Whitehall and more broadly embedded into the Civil Service to support government decision-making and the implementation of systems thinking within resilience planning.
   - Diversity of experience and expertise should be an active consideration when planning for emergencies and resilience, as a wider range of perspectives will enable better understanding of potential impacts on marginalised and vulnerable groups and stimulate the introduction of new and innovative ways of tackling complex challenges.

2. **Government should undertake an audit to map existing public, private and third sector capabilities and convening bodies against the critical capability groups. This will help build a better understanding of how these organisations and their capabilities can be best deployed to support future emergency response. The audit should be led by the Cabinet Office Civil Contingencies Secretariat (CCS), in partnership with Government Office for Science (GO-Science), devolved administrations and departmental resilience teams responsible for the risks in the National Risk Register (NRR). An aim of the audit should include developing a reporting framework to engage the private sector and build a practical mechanism to keep the audit as live as possible**.
   The audit should inform the following areas:
   - Strategic workforce planning and the skills and training pipeline for resilience in both the public and private sector.
   - Investment in resilience, including clarity of ownership and roles in the Civil Service, public sector research establishments (PSREs), regulators and coordination to leverage industry investment in resilience.
   - Mapping of the national and international networks that already exist, gaps and crucial point contacts.

3. **The CCS, in partnership with GO-Science, should work with the Royal Academy of Engineering and others to develop the critical capabilities approach into a practical tool for emergency planning, preparedness and resilience that builds on existing capabilities programmes. This should include embedding the practices for preparedness alongside current foresight and horizon scanning methods and exercises. This will identify and ensure the right capabilities are in place to respond effectively and with agility to future scenarios and risks**.
   - Risk owners in government should increase the extent and realism of exercises carried out, drawing on the wider capabilities identified in the audit to support the proactive building of networks ahead of time. This should consider participation, frequency, scenario characteristics (scale, location, severity), how much warning is provided and the mechanisms for activating emergency measures. Outcomes should be shared with teams or organisations responsible for mitigation strategies, and regular reviews should be put in place to monitor implementation of lessons.
   - This recommendation directly supports government's priority actions outlined in the Integrated Review to improve our ability to test and develop our capabilities through contingency planning and regular exercises, bringing together government, the emergency services, the armed forces, other local responders and industry. It can support the national resilience strategy work that is already underway.

Introduction

The COVID-19 context: project instigation

The COVID-19 pandemic has brought the issue of interconnectedness to the fore and highlighted certain vulnerabilities resulting from local, national and global disruptions. For example, the shocks to complex international supply chains resulted in shortages in critical supplies such as personal protective equipment (PPE) and chemical reagents for testing. These disruptions have resulted from a combination of increased demands, international material shortages, and disrupted transport and logistics due to trade restrictions and costs[1].

Despite these challenges, there are many examples of successful mobilisation of UK capability. Examples include the UK's research and innovation base responding at exceptional pace to develop a range of testing methods, vaccines and rapidly manufactured critical care equipment[2]; individual industrial sectors such as telecommunications and energy successfully adapting to a sudden change in demand, working with allied service providers to ensure connectivity and supply are maintained; the repurposing of manufacturing capability and capacity from engineering companies to meet NHS ventilator demand[3]; and the mobilisation of individuals that has enabled immediate local responses to support those who are vulnerable and to overcome central distribution challenges.

This report examines how a wider systems approach to emergency planning and capabilities can enable the UK to better prepare and respond to future emergencies, grounded in evidence from past emergencies. This is not a study of the COVID-19 emergency: the pandemic is ongoing and its full lessons will take time to learn. But COVID-19 acts as a live reminder that emergencies do happen, and while preventative measures can be taken to lessen their likelihood, how well we respond to them depends heavily on the capabilities in place. As the risks of emergencies and threats evolve, as well as the capabilities at the UK's disposal to respond, it is crucial to consider how resilience can be improved in preparation for future challenges and their uncertainties.

How an engineering perspective can help

Engineering plays a vital role in making things work, or making things work better. This includes practical design based on user needs, scalability to meet demand, and balancing safety, sustainability, resilience, and affordability of goods and services.

Engineers are trained to develop and examine complex systems, from self-driving cars to a nuclear power station, or a national telecommunications network keeping millions of homes and businesses connected. They assess risk and identify how it might be propagated to ensure the system can continue functioning safely. Engineering professionals make a commitment to honesty and integrity, accuracy and rigour, respect for life, law, the environment and public good, and the promotion of high standards of leadership and communication[4].

We believe engineering habits of mind, illustrated in Figure 3[5], are a vital resource in both chronic and acute emergencies, especially problem finding and definition, creative problem-solving, improving, adapting and systems thinking as well as the habits of collaboration, resourcefulness and resilience.

The Royal Academy of Engineering has the unique ability to be able to bring together a depth of knowledge and expertise on disruptive innovation, technical capabilities, and risk and safety management. With networks that cross companies of all sizes, from multinationals to high-tech startups, professional engineering institutions, and UK government departments and agencies, the Academy is well placed to draw on best practice and cross-sector learning. Deploying a systems approach, this project explores the interconnected critical capabilities required to ensure UK preparedness for and resilience to challenges.

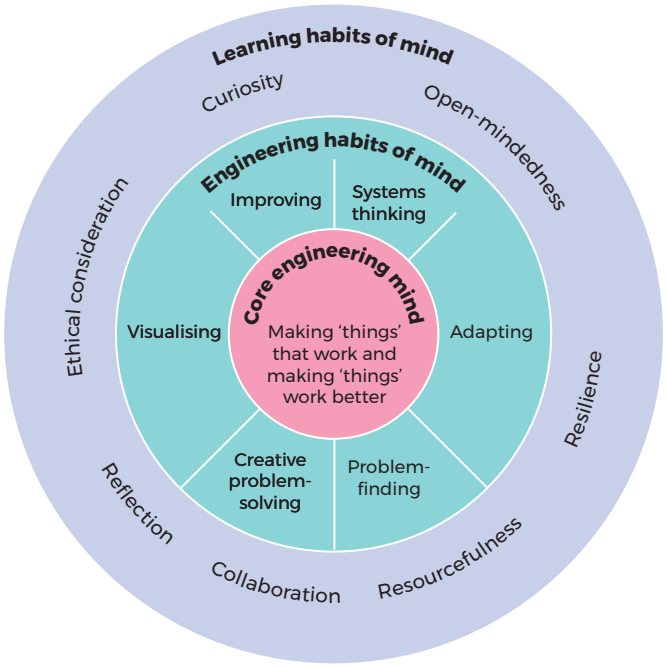


Figure 3: Thinking like an engineer[5]

Critical capabilities: project aims

Emergency responses draw upon a range of capabilities – **the people, infrastructure and assets that need to be available and rapidly mobilised for an effective response. These are essential for an effective national response to an emergency or crisis and for strengthening long-term resilience within an increasingly interconnected world. We have termed these 'critical capabilities'**.

The critical capabilities project aims to explore how a wider, systems-based view of the elements of an emergency response can enhance the current approach to planning, preparedness and emergency response. Studying past emergencies provides a lens to identify the capabilities that enabled resilience and weaknesses that disrupted the response, and the networks and co-ordination that connected them. It highlights common practices that increase preparedness, and which help to prevent cascading failures and improve the ability to quickly recover or adapt (Figure 4).

Project scope

The Integrated Review calls for a 'whole-of-society' approach to resilience, so that individuals, businesses and organisations all play a part in building resilience across the UK. This report proposes a broad capability lens to emergency preparedness. This was validated through the exploration of four past emergencies, **with a particular spotlight on networks and coordination capabilities** that bring together the critical capabilities required in an emergency response. The cross-cutting lessons have informed **practices for preparedness** that should be embedded into future scenario preparedness and emergency response planning, and **recommendations for government** on strengthening systems thinking within government in applying those practices and working in partnership with engineers to support the development of the national resilience strategy work which is already underway.

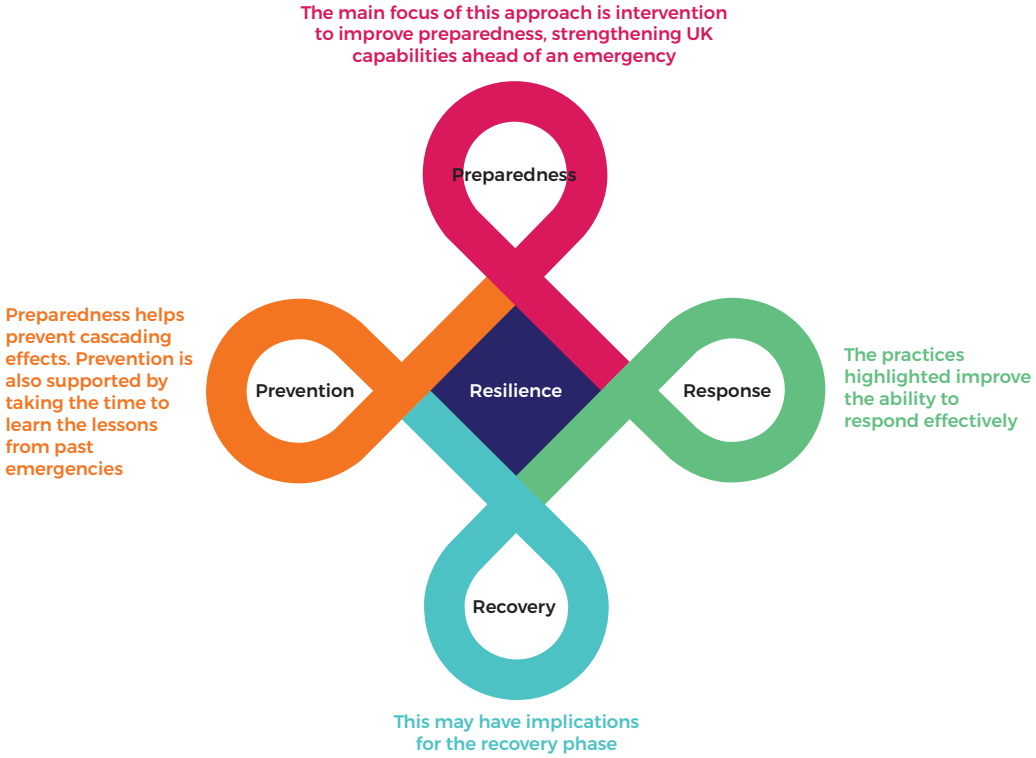


Figure 4: Role of the critical capabilities approach in emergency preparedness and response

This report does not offer comment on the effectiveness of the response to the COVID-19 pandemic, as this remains a very live emergency.

Although where applicable, COVID-19 examples have been included to further illustrate critical capabilities in a current context.

Resilience has a range of definitions. Across this report, the definitions used are the following:

Resilience: the ability to anticipate, resist, absorb, recover, and adapt to shocks and stresses in the system with agility. System resilience is the continuity of delivery of critical needs, including safety, food, transport, energy, and healthcare.

Preparedness: actions taken in anticipation of an emergency to facilitate rapid, effective and appropriate response to the situation. This is the focus of this work.

Prevention: natural hazards often cannot be prevented. However, measures to mitigate those human-introduced vulnerabilities that have the potential to compound impact of a natural hazard are included within the preparedness approach of this work.

Recovery and adaptation: acknowledging the dynamicity of the system, resilience must include the agility to adapt, rather than exclusively aim to return to a previous state.

People, skills and relationships within and across organisations were highlighted as crucial to emergency response

The wider context: UK approaches to emergency response and preparedness

Public and private sector approaches to emergency preparedness and response were explored through desk research, and interviews with government departments, and UK and international industries. The structures and frameworks for UK emergency response and preparedness are outlined alongside some identified limitations.

The legal framework

In the UK, the framework for emergency planning and response is outlined in the **Civil Contingencies Act** (2004)[6,7]. The Act outlines the roles and responsibilities of those involved in emergency preparation and response, as well as good practice and guidance. The Act can also be used to provide emergency powers to the executive, although this has not been used to date, instead specific-to-the-emergency legislation has been passed in UK Parliament, such as the Coronavirus Act (2020)[8].

Risk identification

The NRR is a public document that identifies the environmental hazards, human and animal health, major accidents, societal risk, and malicious attacks that could happen in the UK, presenting their potential likelihood and impact[9,10]. These include hazards such as flooding, disease or space weather events. It is refreshed every two years and is based on the classified **National Security Risk Assessment (NSRA)**, which rigorously assesses risks that will seriously impact the UK. The NRR and the NSRA inform local risk registers and highlight a series of emergencies based upon likelihood and impact, that the UK needs to prepare for.

Government departments: roles and responsibilities

The **CCS** in the Cabinet Office leads the UK government's work in planning and preparing for emergencies. Planning for emergencies is similar in Wales compared to England, whereas Scotland and Northern Ireland have different frameworks[11].

CCS is responsible for coordinating the review and updating NSRA and the NRR every two years. CCS has a **list of critical capabilities for emergency response, which includes, for example, dealing with mass casualties**. The areas underpinning each capability include plans and procedures, personnel, legislation, infrastructure, information, training, and exercise. **The focus is predominantly on the public sector, while maintaining some visibility of the private sector**.

Each risk in the NRR is assigned to a **lead government department**, responsible for more detailed planning and leading the emergency response (depending on severity)[12]. As part of the planning, a '**reasonable worst-case scenario**' **(RWCS)** is generated for each risk. The RWCS is intended as a worst plausible manifestation for a particular emergency; an illustration of a high threshold for preparation. It defines the proportionate preparation of capabilities needed for the range of possible emergencies arising from a threat or hazard[13].

GO-Science advises on the methodology and support the NSRA process. They provide support on sourcing the right science advice and identifying experts for the NSRA's risks and works with the risk-owning departments to understand technical knowledge or capability gaps. GO-Science also organises exercises to prepare and practice for the operation of the **Scientific Advice Group in Emergencies (SAGE)**, chaired by the Government Chief Scientific Adviser[14].

The **Ministry of Defence (MoD)** can be brought in to support an emergency response, although this is viewed as a last resort[15].

The resilience team in the **Ministry for Housing, Communities and Local Government (MHCLG)** act as a central link to **local resilience forums (LRFs)**, which coordinate the on the ground response.

Local response

Most emergencies are managed at the local level. Depending on their nature and impact, the responsibility of leading the emergency response may escalate up to a lead government department. For major emergencies where a cross-departmental response is required, a **Cabinet Office Briefing Room (COBR)** meeting is initiated to enable coordination and decision-making at the ministerial level[16]. Gold-Silver-Bronze Command structures, similar to those used in the military, are often deployed to effectively manage the response.

LRFs bring together the local organisations at the core of the response for most emergencies[17]. There are 38 in England, defined across policing areas, and four in Wales while Scotland and Northern Ireland regional resilience partnerships and emergency preparedness groups carry out similar functions[18]. Their membership includes the emergency services, local authorities and NHS bodies. Individually these organisations (**Category 1 responders**) are required to assess and communicate the risk of emergencies occurring, put in place emergency and business continuity plans, and cooperate with and assist other responders. The LRF brings them together to share information and write the local risk assessment. 'Cooperating' organisations (**Category 2 responders**), for example utility providers or the Health and Safety Executive, have a responsibility to work with and share information with Category 1 responders and may attend some LRF meetings.

Each LRF operates in its own way[19] and, depending on their geography, have different levels of experience in managing certain emergencies such as flooding. They are not a governing body and do not have a budget to work with, or mandated standards or common frameworks to operate within. Some LRFs collaborate and there are data-sharing platforms and MHCLG advisors to facilitate the sharing of good practice.

Emergency planning and response in the private sector

Business continuity plans detail the procedures to ensure operations and service delivery continue during a disruption. These plans are established practice in both the public and private sector.

In the private sector, business continuity plans represent the bulk of resilience planning for emergencies. The operational structure will depend on the company, sector, its size and geographic spread. Safety-critical industries, such as nuclear power or chemicals for example, have specific approaches to risk management. In the case of the nuclear industry, the focus is on safety critical roles and the 'defence-in-depth' model, with multiple layers of hazard mitigation[20].

Practising emergency responses

In both the public and private sector, **exercises** are viewed as key to pressure test, identify gaps and vulnerabilities, and understand where accountability and oversight lie. People, skills and relationships within and across organisations were highlighted as crucial to emergency response. Exercises provide the opportunity to train the personnel who will play a part in an emergency response and to build the skills required. In some cases, the exercises were described as a useful tool to identify those personnel who are best at managing the high intensity and uncertainty of emergencies and ensure they are positioned to be 'in the right place at the right time'. There are practical challenges to exercises, including the choice and design of scenarios, the breadth of individuals and organisations involved, and the cost, logistics and planning required to do this well and at scale. The COVID-19 pandemic has impacted on organisations' ability to run these previously large in-person events.

Limitations of the current approach

The UK's approach to emergency preparedness and response, including the NRR, is generally viewed internationally as leading practice[21]. The involvement of a range of experts, production of a publicly available risk register and frameworks enabling flexibility in the response have been noted as good practice.

However, there are some limitations and challenges that were identified in desk research and the interviews conducted with people involved in emergency planning and response. These include:

- **The interface between the public and the private sector**: although this is considered in the emergency planning process by CCS and government departments, it does not always lead to a good understanding or visibility of each other's capabilities. The complexity and diverse landscape of LRFs can be challenging for the private sector to engage with, for example for information and data sharing. Other tools for preparedness, for example live exercises run by the public sector, predominantly include emergency and first responders. Private sector participation is often limited to utility providers and critical national infrastructure, and so building links across broader networks can be challenging.

- The planning process does aim to take a holistic view of the system by using exercises, systems mapping and information sharing across organisations to capture interdependencies[22] and the risk of cascading failure. However, **interdependencies, concurrent risk, residual risk and cascading failure** were viewed as areas that would benefit from improved consideration during planning.

- **Ownership of risk**: individual risks are assigned to different lead government departments to prepare for. However, several examples were identified where overlapping risks or concurrent risks resulted in a lack of clarity about who was accountable for the response. There can be a disconnect between those who own the risk and need to put mitigation plans in place and the availability of support to fund these mitigation plans.

- **Ownership of resources**: there are different approaches to ownership of response capability across government. The MoD prioritises ownership of resources for resilience, in part for ease and security of access. In contrast local councils, which are a key element of the emergency response framework, currently do not necessarily own many of the facilities or services that may be deployed during an emergency response, rather these are usually contracted out. In this case, procurement processes, availability and prioritisation for deployment become key. Both approaches present benefits and trade-offs and highlight the importance of the public–private interface in emergency situations.

- **The case for investing in resilience**: resilience is often framed as a cost and seen as a trade-off against efficiency, despite its wider benefits. A key question continues to be how to make the case to government to 'buy the insurance'.

The case for investing in resilience

One of the most crucial challenges raised in evidence gathering was 'making the case for insurance' for government to invest in resilience. However, where there lies a cost to investing in resilience, this investment can deliver strong co-benefits to the UK's global competitiveness.

Past emergencies show the importance of resilience, which often comes at a cost and needs to be weighed up against competing priorities such as efficiency. This cost could be in the form of building in redundancy – having a 'spare' capacity or capability where failure is unacceptable, or a piece of infrastructure used only in the event of an emergency, for example a back-up communication system or specialist equipment such as an aircraft that will only fly in the event of an ash cloud. There may be few co-benefits, and the conspicuously high costs must be balanced with the likelihood and extremity of the reasonable worst-case scenario to judge whether or not it is value for money.

In other cases, the cost, while high, may bring strong co-benefits. Investing in specialist skills or industrial capacity and manufacturing capability may have strong economic and social co-benefits. When resilience comes from an enhanced capacity to adapt and be more agile, for example where facilities or equipment is designed to be flexible or adaptable from the start or people are continually being upskilled and able to be redeployed, the investment may be more modest and could instead bring substantial benefits to the UK's competitiveness.

These decisions involve difficult trade-offs, and a systems view may help to identify these trade-offs more easily. By taking a capability-led approach encompassing the public and private sector, this report hopes to highlight those capabilities that are crucial to emergency response and that require long-term and sustainable investment. For example, skills, research and innovation, international partnerships and industrial capability are all capability areas that need to be built up over time. They are also capabilities that underpin economic growth and a thriving knowledge economy.

The critical capabilities approach

Figure 5: Critical capabilities

Introducing critical capabilities

The UK's approach to emergency planning and preparedness provides a strong framework for risk assessment and response but does have limitations. This report explores how a broader capability-led approach to examine emergency preparedness may complement existing practices.

Critical capabilities include the people, infrastructure and assets essential for an effective national response to an emergency or crisis and strengthening long-term resilience within an interconnected world. Six intrinsically interdependent groups have been identified, illustrated in Figure 5: research and innovation; national assets; industrial capability; skills and labour; and resources; with networks and coordination capabilities bringing together the capabilities required to respond to a specific emergency. These capability groups are defined to capture the breadth and diversity of capability available to the UK and essential to respond to emergencies.

The Integrated Review calls for a whole-of-society approach to resilience, so that individuals, businesses, and organisations all play a part in building resilience across the UK. The critical capabilities approach provides a way to consider the interconnected and interdependent nature of each capability group. This systems approach will identify the strong foundation of capabilities already available in the UK or accessible through our international networks so they can be strengthened and exploited.

What is a systems approach?
A systems approach can encourage evidence gathering that draws upon the widest, most diverse and critical perspectives leading to a 'bigger picture' view of the system and its actors. It can help to understand the complex interactions enabling a greater understanding of the implications of each change or decision on the challenge as a whole.

The Critical Capability Groups

Resources includes the data, materials, components, or funds always needed, including in a crisis or emergency. These are underpinned by international market and trading relationships. Examples include sandbags, operations rooms, 4x4s, stocks, information, and guidance.

Skills and labour includes the education, training and diverse workforce who are able and available to underpin the other capability groups. Examples include people power, the armed forces, cybersecurity professionals or other expert skills, and training providers.

Research and innovation includes the facilities and people able to provide expertise, build an understanding of emerging challenges, and discover, develop and scale innovative solutions and enterprises in response to a crisis or emergency. Examples include universities, startups, international research centres, national laboratories, and Catapult Centres.

Industrial capability includes private sector capacity and ability to analyse, manufacture, construct, produce, repurpose, or redeploy if needed, and always deliver key components or items. Examples include the manufacturing industry, technology businesses, airlines, and logistics.

National assets include the physical and digital infrastructure to deliver critical needs such as telecommunications, energy, water, transport, healthcare, security, and safety. Examples include the NHS, regulators, the Met Office, utility providers, Public Health England, National Academies, and government departments.

Networks and coordination capabilities include those existing or transient networks that are in place to enable effective communication, rapid mobilisation of expertise or facilitate effective coordination between stakeholders in government and industry in response to a crisis or emergency. Examples include SAGE, local resilience forums or NHS Emergency Preparedness, Resilience and Response (EPRR) teams.

Learning from past emergencies: method

Case studies provide an opportunity to evidence and validate the above framework, and a chance to understand availability and ability for these critical capabilities to be deployed in response to and recovery from an emergency. The initial focus was on '**networks and coordination' capabilities, those capabilities that can enable effective communication, coordination of actors locally, nationally and internationally, access to expert advice, rapid mobilisation of capabilities or engaging the private sector in response to a crisis or emergency**. The networks and coordination capability lens is useful for highlighting the interconnections across the critical capability groups.

Case studies were used to:

- identify, define and understand 'networks and coordination' capabilities, and how they interconnect across the critical capability groups
- understand enabling factors and interdependencies between 'networks and coordination' capabilities and the other capability groups
- learn from past emergencies the challenges and successes in the response at the time and measures introduced subsequently to improve preparedness
- test the critical capabilities approach, including identifying gaps, opportunities and potential limitations.

Table 1: Case study characteristics

	Geographical impact	Acute chronic	Physical digital
Eyjafjallajökull	International	Acute	Physical
UK response to Fukushima	National (Japan) with potential for international	Acute	Physical
Lancaster floods	Local	Acute flood, chronic vulnerabilities to loss of power	Physical
WannaCry	International	Acute attack, chronic vulnerabilities in IT systems	Digital

The four case studies outlined in Table 1 were chosen to cover a range of emergency characteristics including geographic impact of the emergency (international, national or local), and type of emergency (acute or including chronic vulnerabilities, physical or digital).

A further benefit of using these case studies is that they were relatively well documented. Desk research, including national inquiry reports and their underpinning evidence, and other published reviews of the incident management, allowed an initial outline of how the capabilities were deployed in the UK response. Consideration of a range of sources flagged tensions that were then explored further in workshops. Bringing together lessons from four very different emergencies enabled the development of more generally applicable findings, referred to as practices for preparedness, for organisations in the public, private and third sectors.

Building a narrative helped to identify how network and coordination capabilities were deployed in practice to the response. Using the networking and coordination capability lens identified the key stakeholders (actors) to understand how they were interconnected and to see how they drew on the other capability groups: research and innovation, national assets, industrial capability, skills and labour, and resources. **This approach was not intended to provide a fully comprehensive overview of the emergency**.

Workshops in late October and November 2020 brought together participants with direct experience of each case study emergency response or relevant expertise to revisit the UK response. The discussions helped to verify our presentation of events and to explore key themes around capabilities and the benefit of hindsight, drawing out what would have enabled a better response at the time and UK preparedness to respond to the same emergency now. While there are limitations to relying on personal accounts of events that rely on memory recall sometime after the event, bringing together diverse perspectives enabled us to explore areas of agreement and divergence. When stakeholders were unable to contribute directly to the project, we used published reports as a supplementary source of information.

The case studies we have selected are complex events and are presented in this report in a condensed format, which doesn't capture every single detail but provides an overview of the key events, stakeholders and different elements of the emergency responses.

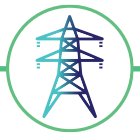
Introduction to case studies

The four case studies outlined below were chosen to reflect a range of emergency characteristics (physical/digital disruption, central/local coordination and national/international impact), test and build a broad understanding of the critical capability groups, and identify cross cutting lessons.

Further detail of these case studies is available in **Annex A**.

Eyjafjallajökull volcano eruption in 2010
On 20 March 2010, the Icelandic volcano Eyjafjallajökull began an initial eruption, followed by a second eruption starting on 14 April 2010. From 15 to 20 April 2010, ash from the volcanic eruption covered large areas of Northern Europe, resulting in countries closing their airspace. 104,000 flights were cancelled during an eight-day period, 48% of total air traffic, affecting millions of passengers globally[23,24,25]. Volcanic activity and ash advisories for areas of ash affecting flights continued to be issued until 23 May 2010.

UK response to the Fukushima nuclear accident in 2011
On 11 March 2011, a severe nuclear accident happened at the Fukushima Daiichi Nuclear Power Plant in Japan. An earthquake-triggered tsunami flooded the power plant's lower grounds damaging the emergency generators which the plant was relying on to power the pumps circulating coolant. The loss of coolant led to three nuclear meltdowns, three hydrogen explosions and the release of radioactive contamination.



Lancaster flooding leading to loss of electricity in 2015
On 5 December 2015, flooding from Storm Desmond led to the loss of electricity supply to 61,000 properties in Lancaster[26,27]. The situation returned to relative normality by 11 December. 75 large diesel generators were brought from across the country to restore supply, but a second fault created additional delays in restoring electricity. Loss of electricity resulted in loss of communications. Schools, retail, rail travel were disrupted. The local hospital has back-up generators but that wasn't the case for care facilities.

WannaCry ransomware incident affecting NHS in 2017
On 12 May 2017, a global ransomware attack, known as WannaCry, affected more than 230,000 computers in at least 150 countries. Although not directly aimed at the NHS, 34 trusts were infected and 46 were affected resulting in 30,500 cancelled appointments and 595 GP services impacted. The incident lasted a week until 19 May 2017. Five acute trusts were diverting patients from their A&E departments and a number of trusts were experiencing issues with diagnostic services leading to cancelled appointments and procedures[28].

Spotlight on networks and coordination capabilities

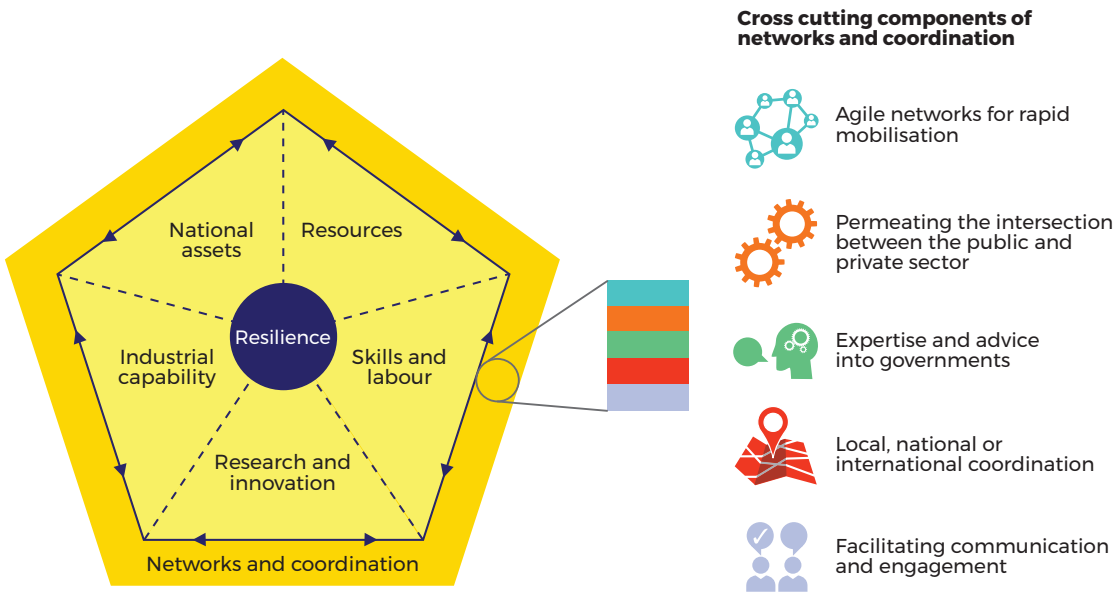


Figure 6: The critical capabilities and cross-cutting components of networks and coordination

Networks and coordination capabilities bring together the capabilities that are needed to provide an effective emergency response. This report focuses on this capability group as it provides an overview across all critical capabilities and their interdependencies. In operational terms, networks and coordination capability is essential to effectively prepare and respond to an emergency at pace and to navigate the uncertainty as the emergency emerges and unfolds.

Exploring networks and coordination capabilities was also a means to bring international considerations to the foreground. Whether the potential impacts of an emergency that occurs in a different country such as the Fukushima nuclear accident, natural hazards unbounded by national borders and the risks from increasing reliance on global supply chains, the world is increasingly connected and we are only as resilient as the weakest link.

Five components of networks and coordination capability were highlighted across the case studies and are illustrated in Figure 6:

- **Agile networks for rapid mobilisation**: the capability to rapidly activate, assemble and coordinate a network of organisations and people to effectively deliver the components of the emergency response concurrently.
- **Permeating the intersection between the public and private sector**: the capability to coordinate networks bringing together public and private sector capabilities and capacity to effectively deliver the emergency response.
- **Expertise and advice into governments**: the capability to provide summaries of emerging evidence, communicate uncertainty and collate input from those on the ground to answer governments questions and inform decision-making.

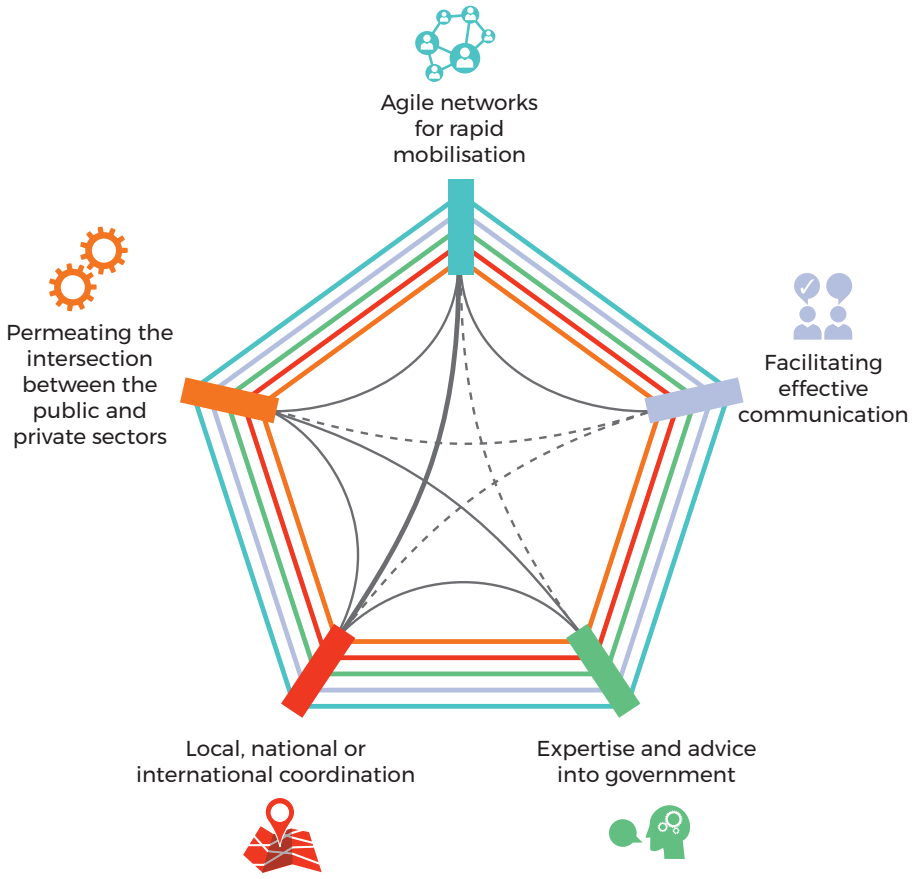


Figure 7: The interconnected networks and coordination capabilities. The weight of the line between the components signifies the frequency these components of networks and coordination capability were reliant on each other in the responses presented in the four case studies

Local, national or international coordination: the capability to bring together a coordinated response with a network spanning a geographic footprint or scale – local, national and international.

Facilitating effective communication: the capability for effective exchange of information, uncertainties and concerns with key stakeholders, including businesses and the public, to facilitate an effective emergency response.

Testing with the case studies

In emergency response, networks and coordination capabilities draw on each other. The case studies provided illustrative examples of this interconnectedness, illustrated in Figure 7.
For each case study, an example of each of the components of networks and coordination has been drawn out. The connections with the other cross-cutting components of networks and coordination have been identified, exploring how they draw upon the underpinning critical capability groups of skills and labour, resources, research

and innovation, national assets, and industrial capability to respond. The success of each part of the response relied heavily on the roles different networks and coordination capabilities played. In each case the national assets, which include central government departments and arms-length bodies, played a critical coordination role, drawing together the skills and resources needed and leveraging industry and research and innovation capabilities.

For each component of networks and coordination capability, we identified key learnings by bringing together the wider insights from the four case studies. These learnings are not intended to be comprehensive and will be limited by the choice of case studies, the specifics of each emergency and the stakeholders involved. However, the trends that emerged provide a basis to build upon for improving networks and coordination capabilities in the UK.

Eyjafjallajökull volcanic eruption

On 20 March 2010, the Icelandic volcano Eyjafjallajökull began an initial eruption, followed by a second eruption starting on 14 April 2010. From 15 to 20 April 2010, ash from the volcanic eruption covered large areas of Northern Europe, resulting in countries closing their airspace. 104,000 flights were cancelled during an eight-day period, 48% of total air traffic, affecting millions of passengers globally[29,30,31]. Volcanic activity and ash advisories for areas of ash affecting flights continued to be issued until 23 May 2010.

Component of networks and coordination capability	Example	Links to networks and coordination capability components	Links to critical capability groups
Agile networks for rapid mobilisation	The regulators initially needed to know location of the ash cloud to identify safe flight zones. This evolved to concentration of ash as the regulations changed. The Met Office provided regular forecasting of the ash cloud location. This required data from satellites, monitoring stations and from close proximity to the volcano as inputs into the Numerical Atmospheric-dispersion Modelling Environment (NAME) model. Delays to the deployment of the UK airborne research aircraft created challenges.	International coordination for the collection of NAME model input data from monitoring stations in Iceland, the UK and across Europe, drawing on existing research and national weather service collaborations. The Met Office and British Geological Survey provided regular updates to SAGE, devolved authorities, the Public Health Authority (now Public Health England), and the Civil Aviation Authority (CAA).	National assets: the Met Office, regulators and the MoD. Research and innovation (R&I): NERC, BGS and universities with the research skills and equipment. Skills: modelling, volcanology and atmospheric sciences. Resources: models, data, measurement equipment, satellites, and research airplanes.

continued over...

Component of networks and coordination capability	Example	Links to networks and coordination capability components	Links to critical capability groups
Permeating the intersection between the public and private sector	To develop ash safety regulation, the CAA worked with the Met Office, SAGE, aircraft engine manufacturers, the airline industry, and international regulators. Bringing public and private sector perspectives together allowed the allowed ash concentrations for safe commercial flight to be defined.	Agile international networks were assembled to define safe flight regulation in a matter of days. International coordination at pace and effectively across European and North American regulators and industry. Effective communication with videoconferences to bring networks together and briefings for industry. Expert advice with SAGE validating the CAA's work focus and feeding back into government.	National assets: regulators, use of telecommunications. R&I: expertise from meteorologists, volcanologists and geologists, NERC. Industrial capability: expertise from engine manufacturers and coordination with airlines. Resources: lack of evidence of airworthiness of aircraft in ash.
Expertise and advice into governments	SAGE was convened, the initial focus was on health and agriculture impacts, including potential presence of sulphur and risk of a second eruption. Meanwhile flight safety was being assessed through international collaboration lead by the Civil Aviation Authority (CAA). As the focus of SAGE became flight safety the CAA were a critical participant.	International coordination on safety considerations with CAA, International Civil Aviation Organization, European Union Aviation Safety Agency, and Eurocontrol and input from Icelandic Meteorological Office and researchers. CAA provided a connection to aerospace manufacturers and engineers who weren't included on SAGE.	National assets: Met Office, CAA, government officials. R&I: British Geological Survey, volcanologists, meteorologists, NERC.

Component of networks and coordination capability	Example	Links to networks and coordination capability components	Links to critical capability groups
Local, national or international coordination	The UK's CAA led the efforts working with European, North American, and other international regulators and organisations to define ash concentrations for safe flight zones and enable the safe reopening of airspace.	Agile networks, largely built on existing relationships, were mobilised through videoconferences for input. Permeating the public/private interface with input from industry and regulators. Effective communication was challenging because of the different interpretations of the regulation in place and briefings for industry were supported by SAGE. Expert advice into government provided via exchanges with SAGE and liaison with the Department for Transport (DfT).	Skills: aerospace engineering, meteorology and dispersion, volcanology, air traffic and airspace management. R&I: developing the understanding of airworthiness of aircraft in ash. Industrial capability: engine manufacturers and airlines. National assets: CAA and regulators (both military and civil).
Facilitating effective communication	Communication was challenging with the press and between the regulator and airline industry.	Agile networks faced challenging communication with some organisations. Permeating the public/private interface with challenging communication channels between the public sector bodies and industry.	National assets: government officials, CAA. Industrial capability: aerospace manufacturers and airlines.

UK response to Fukushima nuclear accident

On 11 March 2011, a severe nuclear accident happened at the Fukushima Daiichi Nuclear Power Plant in Japan. An earthquake-triggered tsunami flooded the power plant's lower grounds damaging the emergency generators, which the plant was relying on to power the pumps circulating coolant. The loss of coolant led to three nuclear meltdowns, three hydrogen explosions and the release of radioactive contamination.

Component of networks and coordination capability	Example	Links to networks and coordination capability components	Links to critical capability groups
Agile networks for rapid mobilisation	Staff at the British Embassy in Tokyo, unaffected by the earthquake, were mobilised to form a crisis response centre to guide relief efforts, including search capability, communication and support to UK citizens.	International coordination with close connection between the Japanese and British governments and national coordination between the Met Office and Health Protection Agency enabled modelled advice to be compiled. Effective communication with the establishment of a hotline to provide advice and support to UK citizens.	National assets: Foreign and Commonwealth Office (FCO) and embassy. Resources: databases, information gathering and search capabilities, atmospheric and health impact models.
Permeating the intersection between the public and private sector	Industry supported the efforts of SAGE with knowledge sharing and international evidence collection. Industry then played an important role in the subsequent recovery and adaptation, including reviewing and implementing safety lessons at UK power plants.	Expert advice with industry expertise on reactions drawn upon and used to verify calculations. International coordination provided access to information.	Industrial capability: implemented the learnings from Fukushima. Resources: information about the reactors.

Component of networks and coordination capability	Example	Links to networks and coordination capability components	Links to critical capability groups
Expertise and advice into governments	Through SAGE, the radiation, chemical and environmental hazards were assessed by an expert group and the Met Office assessed the weather implications for Tokyo and potential risk to health with Public Health England. The US Chief Science Advisor and head of the nuclear authority provided verification of calculations.	Agile networks for mobilisation included joint agency modelling capabilities to provide useful information on risk to health. International coordination provided access to information and verification from other experts.	National Assets: Met Office, Public Health England, MoD, Office for Nuclear Regulation, FCO. R&I: National Nuclear Laboratory, researchers. Industrial capability: Sellafield.
Local, national or international coordination	International networks and connections were used to gather information about the Tokyo Electric Power Company (TEPCO) plant and to verify UK analysis.	Expert advice provided through strong international links through SAGE members' networks.	Skills: international nuclear expertise. Resources: directory of contacts and access to information.
Facilitating effective communication	Considered communication of the scientific evidence through press conferences for UK citizens in Japan helped allay panic.	Expert advice with SAGE providing confidence in messaging. International coordination with two-way communication with people on the ground.	National assets: FCO, British Embassy and Science Media Centre enabled effective communication. Resources: relied on data and information to draw conclusions.

Lancaster flooding leading to loss of electricity

On 5 December 2015, flooding from Storm Desmond led to the loss of electricity supply to 61,000 properties in Lancaster[32,33]. The situation returned to relative normality by 11 December. 75 large diesel generators were brought from across the country to restore supply, but a second fault created additional delays in restoring electricity. Loss of electricity resulted in loss of communications. Schools, retail, rail travel were disrupted. The local hospital has back-up generators but that wasn't the case for care facilities.

Component of networks and coordination capability	Example	Links to networks and coordination capability components	Links to critical capability groups
Agile networks for rapid mobilisation	Local community initiatives were deployed across Lancaster to provide free hot food. The police were drafted in from surrounding areas to help local services contact vulnerable people.	Local coordination with different third sector organisations and businesses to provide support to the affected communities.	National assets: police. Resources: food, power source for cooking such as a campervan, data on potentially vulnerable people. Skills: police, staff and volunteers to support the effort.
Permeating the intersection between the public and private sector	Only one supermarket in the Lancaster area had a rented generator and was able to open during the power cut. Despite high demand, the store had to close at 4.00pm to respect Sunday trading rules. The local council managed the additional waste from hospitality and retail as perishables could not be kept safely refrigerated.	Agile networks for mobilisation with additional local staff brought in to manage the high demand at the supermarket.	National assets: card payments were not possible without the internet, but the ATM was working as it used a phone line and did not run out of cash. Skills: additional staff. Resources: back-up generator.
Expertise and advice into governments	The Environment Agency and the Met Office issue publicly available weather and flood warnings and forecasts. There were no specific examples of expert advice into the local government for the Lancaster case study.	Effective communications including forecasts and resources for emergency responders and local authorities.	National Assets: Environment Agency, Natural Resources Wales, Met Office. Skills: meteorology, modelling, hydrology.
Local, national or international coordination	Electricity North West (ENWL) brought in 75 large generators from across the UK to reconnect 22,000 customers the following day.	Agile networks for mobilisation provided generators to ENWL.	National asset: Fire brigade, ENWL. Resources: generators, pumps. Skills: electrical engineering.

Component of networks and coordination capability	Example	Links to networks and coordination capability components	Links to critical capability groups
Facilitating effective communication	Loss of communications led to the local hospital becoming an information hub. Information was relayed in several ways, including the local radio station, Bay radio, paper signs placed outside the schools to announce closure and word of mouth. This was not necessarily coordinated with the emergency response leading to misinformation. The local council were able to use the LRF communication system.	Agile networks for mobilisation were initially mostly composed of people from outside the affected area who still had telecommunications. Permeating the public/private interface with the local radio station becoming an important source of information. Local coordination was challenging without communication, especially for headteachers who didn't receive briefings.	National assets: loss of communications, BBC radio. Industrial capability: Bay radio. Skills: radio operators. Resources: LRF phone.

WannaCry ransomware incident affecting NHS in 2017

On 12 May 2017, a global ransomware attack, known as WannaCry, affected more than 230,000 computers in at least 150 countries. Although not directly aimed at the NHS, 34 trusts were infected and 46 were affected resulting in 30,500 cancelled appointments and 595 GP services impacted. The incident lasted a week until 19 May 2017. Five acute trusts were diverting patients from their A&E departments and a number of trusts were experiencing issues with diagnostic services leading to cancelled appointments and procedures.[28]

Component of networks and coordination capability	Example	Links to networks and coordination capability components	Links to critical capability groups
Agile networks for rapid mobilisation	A cross-departmental emergency team was mobilised and led by NHS England/Improvement with a focus on collecting data on affected trusts and ensuring patient safety and continuity of care. As some affected hospitals were not able to provide certain types of care, mutual aid was activated to divert patients and best manage patient care continuity.	National/local coordination with mutual aid and cross-coordination across the NHS. Effective communication to ensure re-routing of ambulances and patients to undisrupted hospitals.	National assets: Department of Health and Social Care, NHS England, local trusts. Resources: access to data and electronic patient records. Skills: operational teams to respond to patient concerns.
Permeating the intersection between the public and private sector	Technical skills in Microsoft provided the required patch and NHS Digital, trust IT teams and equipment manufacturers worked together to apply the patch to disable the ransomware across affected NHS trusts.	National coordination with National Cyber Security Centre (NCSC), NHS England and NHS Digital coordinating. Agile networks for mobilisation were essential to deliver at speed and limit impact on care.	National assets: NHS England and Digital coordinated. Industrial capability: Device manufacturers and IT delivery partners helped with patching. Skills and labour: IT and cyber skills were needed across trusts. R&I: a researcher eventually found the ransomware 'kill switch'.
Expertise and advice into governments	Relationships with Microsoft cybersecurity enabled rapid access to a system patch. GCHQ enabled early awareness and identification of the threat, although this did not provide visibility of the effect on individual NHS trusts.	Communication of the threat in media reports raised greater awareness that resulted in a researcher who was not involved in the response identifying the 'kill switch'.	National assets: GCHQ enabled early awareness. Industrial capability: Microsoft service provision. Skills: need for technical understanding.

Component of networks and coordination capability	Example	Links to networks and coordination capability components	Links to critical capability groups
Local, national or international coordination	The National Crime Agency Centre worked with UK and international partners to share intelligence and coordinate action.	Effective communication both internationally across NCSC, National Crime Agency police, and regional organised crime units.	National assets: Collaboration between NCSC, NCA, police, FCO, and regional organised crime units. Resources: intelligence could have been better shared between organisations earlier to limit confusion.
Facilitating effective communication	Communicating guidance to industry through the Cyber Security Information Sharing Partnership, a joint industry and government initiative set up to exchange cyber threat information to reduce the impact of the attack beyond NHS. Lack of rapid communication early on led to some NHS trusts disconnecting email services to reduce risk but also cutting off communication.	Permeating the public/private interface with a network enabling wider information sharing.	National asset: NCSC coordinating advice. Skills: cyber skills were needed to create guidance. Resources: guidance shared.

Agile networks for rapid mobilisation

Definition: the capability to rapidly activate, assemble and coordinate a network of organisations and people to effectively deliver the components of the emergency response concurrently.

Lessons from the case studies

- The pace and effectiveness of mobilisation is reliant on the relevant organisations, skills and resources being known and available. As such, links between the government and those organisations with known networks of a certain capability are often drawn upon to cascade requests across.

- National assets, which include Public Sector Research Establishments (PSREs) such as the Met Office, play an important role in the mobilisation and coordination of networks. They are reliant on resources, especially data and information, and a highly skilled workforce to deliver. A degree of flexibility and agility, with effective communication, is important to manage changing requirements as the emergency unfolds and requirements evolve.

- Practice and relationship building ahead of time supports rapid mobilisation in the emergency as it builds collective experience and awareness of each other's capabilities and vulnerabilities.

- In an emergency, there is a sense of goodwill that culminates in people and organisations offering help and solutions. However, these offers for support can be challenging to manage and channel into useful responses. Clear points of contact and networks across multiple organisations and the public/private sector interface can be valuable to organise offers of goodwill.

- Loss of communication as seen following the loss of power in Lancaster and disabling of IT systems in WannaCry introduces a significant barrier to effective and rapid mobilisation, which should be accounted for in planning.

An example from COVID-19
Developing and manufacturing medical breathing devices

The need for ventilators for patients critically ill with COVID-19 became clear early in the pandemic. On 16 March 2020, the Prime Minister launched a Ventilator Challenge asking companies to help manufacture, design and build thousands of NHS ventilators. A consortium of significant UK industrial and engineering businesses from across the aerospace, automotive and medical sector was established. The rapid mobilisation of UK manufacturing and research and development facilities meant that, within 12 weeks, they established the capability, supply chains and workforce to create and produce ventilators on a scale that would typically take years[35]. As better understanding of best practice for COVID-19 patient care emerged over time, the urgency of the need for ventilators changed, as non-invasive continuous positive airway pressure (CPAP) was found to be a more effective treatment[36]. The UCL-Ventura breathing aid was developed by UCL engineers, UCLH clinicians and Mercedes-AMG High Performance Powertrains with a first prototype made in just 100 hours; 10,000 breathing aids have been manufactured and are being used in over 130 NHS hospitals[37].

Permeating the intersection between the public and private sector

Definition: the capability to coordinate networks bringing together public and private sector capabilities and capacity to effectively deliver the emergency response.

Lessons from the case studies

- It is important for the public sector to be aware of private sector capabilities and their vulnerabilities, so that this can be mobilised in an emergency response, or to be able to rapidly identify potential impacts that may fall to the public sector to manage. Potential offers of support in an emergency can be missed as time is limited.
- Ownership of the risk and responsibility for emergency response needs to be defined and visible. Better awareness across the public/private interface can enable the private sector to support an effective response.
- Resilience and emergencies should be considered in developing and reviewing regulation and standards, including the potential implications of stating absolute values in regulation. In the Icelandic volcano, the level of ash permitted was defined as zero but no assessment had been carried out to establish a safe level of ash and flight time.
- Legal frameworks, for example data sharing and trading laws, can have a compounding effect in emergencies, as seen in Lancaster with the requirement for the only open supermarket to close despite high demand. Flexibility in such frameworks when responding to an emergency could facilitate an effective response.
- Contracting of public services can fragment the networks that deliver critical services, such as the care sector in the Lancaster case study. LRFs and networks across critical national infrastructure have supported the building and maintaining of links, however gaps still remain.
- Public procurement plays an important role, to establish relationships with contractors and to provide the capability needed in response to an emergency. WannaCry identified the merits of setting up no-value procurement contracts in 'peace time' through a normal competitive tendering process to ensure those capabilities can be drawn upon when needed. Similarly, resilience standards and considerations could be included in contractual obligations for service providers.

An example from COVID-19 Testing

Testing for COVID-19 in the population is pillar two of the Department of Health and Social Care approach to testing scale up and delivered through commercial partnerships during the first months of the emergency. This involved collaboration of Public Health England and the NHS with universities, research institutes and companies such as Randox and Lighthouse Laboratories to establish a network of new labs and testing sites across the UK[38]. Working in partnership has enabled the exchange of staff, equipment, reagents, logistics, knowledge, and skills needed to deliver additional regional testing capabilities of over 500,000 tests a day by 1 March[39]. The results are integrated into the wider NHS Test and Trace system, for which challenges remain[40,41]. Opportunities to maximise resource were identified in an Academy of Medical Sciences report, which included creating opportunities to engage for laboratories outside the process, exploring the value of local approaches and considering timely and long-term workforce and funding for testing capability[42].

Expertise and advice into governments

Definition: the capability to provide summaries of emerging evidence, communicate uncertainty and collate input from those on the ground to answer governments' questions and inform decision-making.

Lessons from the case studies

- Expert advice into government is often drawn in to answer a question, which could be focused around assessing the risk and impact on a population, environment or infrastructure. Defining and refining the question or questions to enable the appropriate focus as early as possible is critical in delivering valuable and timely evidence to inform government decisions. A degree of agility and flexibility is important to respond to the changing needs of the emergency.

- Existing relationships can help with rapid mobilisation of expertise to solve a problem, but a diverse range of experts is important to bring in the breadth of evidence and relevant disciplines in an emergency, including industry, community leaders and social scientists. These lists of identified experts will never be fully comprehensive for the specific emergency so mechanisms that enable input and insights from individuals with valuable expertise that may have been overlooked are required. Communication of the arising issues can allow individuals with specialist skills or perspectives to come forward.

- With any new emergencies, the initial level of uncertainty is likely to be high. As much as the initial decisions in an emergency can shape the direction taken, it is important to encourage review and verify the conclusions experts come to more broadly or internationally. It can be beneficial to have two parallel research responses, one rapid and a second slower-paced response to enable more in-depth research, test initial assumptions and resolve uncertainty as more information becomes available.

- Pre-existing and cross-agency modelling capabilities can enable a rapid initial assessment of the risk. Joint agency modelling is an important capability for ensuring the potential risk is considered more holistically, for example assessment of the health, agricultural and flight risks resulting from the Eyjafjallajökull eruption. Linking and sharing of models ahead of an emergency is an important area of development to facilitate rapid response. For example, the Met Office and the Public Health Authority (now Public Health England) had been working together to join up models that were then used at pace during the response to Fukushima, whereas no direct model to model links existed for impacts of the volcanic ash cloud and expert interpretation was required at the time.

An example from COVID-19
SAGE

Once aware of the scale of the COVID-19 outbreak in Wuhan, Sir Patrick Vallance FRS FMedSci, Government Chief Scientific Adviser, instigated a precautionary SAGE meeting on 22 January 2020 to bring together cross-government expertise[43]. In February, COBR initiated the official formation of SAGE. The membership of the group has evolved with the understanding of the virus, including the formation of eight sub-groups to include wider expertise for the different scientific dimensions of the pandemic[44]. The use of science advice in ministerial decisions or in communications to the public has at times met challenges, including criticisms of the timescales of ministerial decision-making and lack of transparency. However, over 500 papers have been released into the public domain[45,46].

Local, national or international coordination

Definition: the capability to bring together a coordinated response with a network spanning a geographic footprint or scale – local, national and international.

Lessons from the case studies

- Local, national and international networks are particularly important for information, data, knowledge and resource sharing. This coordination often feeds into expert advice into government, rapid mobilisation and the public/private interface.

- The geography of these networks can provide a boost to the capability to respond to emergencies, but also introduces potential barriers especially around data sharing, trust and frameworks for knowledge exchange between different regions, countries and within one country at different levels.

- In the WannaCry case study, international insights were able to identify the ransomware attack ahead of time; as a systems patch had been issued to NHS trusts months earlier the risk of disruption was assumed to be low. However limited patch implementation left the NHS vulnerable. With no clear lines of communication in place, the appropriate advice was not communicated effectively to the local NHS trusts. Since the disruption NHS Digital has shared its experience with the Global Digital Health Partnership, and this exchange of experiences is valuable for wider preparedness.

- Existing frameworks and relationships are crucial to effective coordination in the event of an emergency. At the international level, these are often built through international research and development collaborations and international organisations including UN-associated bodies. In the case of the volcanic ash group, existing groups brought together by the international and European regulators enabled UK leadership and relationships to develop the response to the emergency and establish consensus. Collaborations continued beyond the emergency response.

- Mechanisms such as community groups or LRFs exist to encourage local level engagement. The bridge between national and local coordination is also important, for two-way communication and information exchange especially.

An example from COVID-19
Global vaccine development

On 11 January 2020, the genetic code of the novel COVID-19 virus was published. Since then, the Coalition for Epidemic Preparedness Innovations (CEPI) has led efforts to coordinate international funding of vaccine research and development across a portfolio of vaccine candidates and organisations[47]. CEPI, alongside Gavi, the Vaccine Alliance and WHO, is coordinating COVAX – a platform to support the research, development and manufacturing of a wide range of vaccines with the aim to have two billion doses available by the end of 2021 and ensure access to vaccines for lower-income nations[48,49]. In October, CEPI established a global network for the assessment of COVID-19 vaccine immunogenicity[50]. At the time of writing, the vaccine roll-out is the early stages and it is yet to be seen how rapid distribution will take place across the world, especially to lower-income nations.

Facilitating effective communication

Definition: the capability for effective two-way communication of information, uncertainties and concerns with key stakeholders, including businesses and the public, to facilitate an effective emergency response.

Lessons from the case studies

- Where communication and ability to exchange information fails, it makes effective coordination difficult and raises the importance of multiple communication channels, as seen in the more distributed WannaCry and Lancaster case studies.

- In a disruption there is appetite for information. It is important to fill this with meaningful communications at pace or risk misinformation filling the vacuum; a challenge that is amplified by social media.

- Trust is especially important where international advice diverges. With Fukushima the UK and France agreed on the scientific conclusions but took different approaches to repatriation. Regular and open communication from the UK government Chief Scientific Adviser proved popular with UK citizens and the public in Japan.

- Demographics and behaviours are important to consider, as different population groups will look to different sources of information. This is especially important in emergencies where communications are lost, in which case alternative options such as briefing community leaders ahead of time or knowledge that radios can be a source of information can become crucial and isn't a given, especially with younger generations. These local communications mechanisms can also enable better two-way information exchange.

- In the aftermath of an emergency, honest communication and discussion across the actors and stakeholders in the response are important to learn the wider lessons of the response.

An example from COVID-19
Daily briefings

Downing Street delivered daily briefings to the public from 16 March 2020, including situation updates, announcements and explanation of new measures. The briefings were delivered by different ministers, science and medical advisors, and representatives of bodies involved in the response including Public Health England and the NHS depending on the message of the day. These often included an opportunity for questions from journalists or members of the public, which allowed concerns to be raised and further clarity to be provided. The frequency of the briefings was reduced after 23 June.

The spread of misinformation has been an ongoing challenge. For example, unfounded fears of 5G resulted in damage to antennas, highlighting the importance of clear communication[51]. An Ofcom survey found that 46% of people had encountered false or misleading information about COVID-19 during the last week of March 2020[52].

Summary of the lessons learned

Summary of the lessons on networks and coordination capabilities

Agile networks for rapid mobilisation

Existing networks are required to mobilise capabilities practically, efficiently and effectively in response to an emergency. This relies on a diverse range of specialist skills and equipment, from cybersecurity to having a gas camping stove for cooking without electricity. A central coordinator role typically played by national assets, such as a regulator or the Met Office, provides an important bridge between the public and private sector. These organisations need to be appropriately resourced to maintain this networking capability.

Intersection between private and public sectors

Emergency responses often harness expertise and capabilities from the private sector for skills, expertise, facilities, and information exchange. Effective permeability across the private–public interface with an understanding of what the response requires and what capability the private sector could offer is needed. Where this was used most effectively, it drew on existing relationships or contracts. However, the case studies showed that regulation and laws can cause an unintended cascade of failures. The limitations of regulations in emergencies could be better anticipated and resolved. For emergencies on a large scale, there is a public expectation that government will take action, even if the responsibility for response lies within the private sector.

Expertise and advice into governments

Underpinning expert advice into government requires the availability of experts to bring diverse academic and practitioner perspectives combined with the individual networks they can leverage. The research and innovation community across academia, government, industry and the third sector play an important role. Such expertise requires a pipeline of talent, building careers and specialist knowledge and modelling capability over time. This expert advice often goes hand-in-hand with effective communication, where equipping specialists with skills to communicate with politicians, policymakers and the public is important to ensure complex information can be exchanged and uncertainty conveyed confidently to inform decision-making.

continued over...

Summary of the lessons on networks and coordination capabilities

Local, national or international coordination

Connections at and across the local, national and international levels are an essential component to effective emergency response. These networks serve a multitude of functions, providing an early warning system and supporting mobilisation to solve problems and two-way information exchange both at the time of emergency and after the fact. Existing networks and frameworks for knowledge and data exchange can increase the effectiveness. Coordination and consistency of messaging across different scales or place-based networks can improve the perceived trustworthiness of the response.

Facilitating effective communication

Different communities have different needs, and effective communication relies on a successful assessment of who needs to know what and when. In an emergency, public appetite for information can be high and misinformation can spread at pace. It is vital that informed sources consider the narrative presented. For responders on the ground, clear information flow is critical to understand roles, responsibilities and potential risks that need to be managed. It is important this communication is two-way. Where the emergency disrupts primary communication mechanisms, back-ups, contingency plans must be put in place, whether that's Whatsapp channels, radios or word of mouth.

Practices for preparedness

Reflections on the case study process

The case studies enabled us to do two things. Firstly, we found they extended, shaped and validated our critical capabilities groups. The case studies enhanced understanding of how these capabilities operate within an emergency and to what effect, and viewing these case studies through a capabilities lens structured and enhanced understanding of what happened and the actions that were taken. We are encouraged by this and the recommendations made later include suggestions for embedding a critical capabilities approach into future emergency planning.

Secondly, examination of the case studies yielded specific insights about different practices that can enhance resilience, which is set out later in this section.

There is real value in the benefit of hindsight. The workshop format brought together people involved in the response to the case study emergency; in some cases people who had not met during the emergency but were involved in different aspects of the response or implementation of the arising recommendations. The format enabled a constructive re-telling of the events, highlighting uncertainties and key enablers in the response, which could be mapped back to the critical capability groups. An honest and open discussion around what happened, what had been challenging and what worked well, brought different perspectives to the table.

The forward-looking question regarding what would happen if the same emergency replayed now was not clear cut. This prompted rich discussions about the potential vulnerabilities that might remain or have emerged since, highlighting the importance of dynamic emergency preparedness and interdependencies. Insights from those with lived experience of emergency and response are valuable for understanding the unexpected vulnerabilities that occur. Beyond the essential operational debriefs that take place after an emergency response, government and other organisations may benefit from convening these discussions once some time has passed to reflect more broadly on the challenges and lessons from emergencies. Forums exist both within the UK and internationally, although more can be done to encourage these discussions with broader stakeholder groups and more systematically. While no emergency will ever be the same, some lessons, as highlighted across this report, may have wider applicability for resilience and preparation for the next emergency.

The critical capabilities approach allowed us to really understand what each stakeholder brought to the response and what capabilities were leveraged across which organisations to understand the strengths and weaknesses in the response. The networks and coordination capability lens was an effective mechanism to focus the conversation on the practicalities of deploying an emergency response, the people, organisations and the connections that provide different capabilities. It enabled re-telling and recounting events, and an effective mechanism to compare very different emergencies. The importance of agility and flexibility was highlighted across the four emergencies as similar networks and coordination capabilities were deployed to address different responses, to pull in a range of enabling capabilities and to solve a variety of challenges.

The case studies also provide an insight into the breadth of capabilities and expertise drawn upon for an emergency response – whether a Met Office model, volcanologist with specialist expertise on a particular Icelandic volcano, cybersecurity skills or the availability of generators.

The next steps in this approach may consider taking a focus on a different capability group or looking into future events, while still examining the connections and interdependencies across capabilities. The critical capabilities approach could also be used to explore the response to COVID-19.

Practices for preparedness

By investigating past emergencies through the **cross-cutting lens of networks and coordination capability**, we have identified themes and lessons that could be adopted by public, private and third sector organisations to improve the ability to respond to the next emergency, whatever it entails. While framed as government processes for preparedness, these '**practices for preparedness**' can be applied more widely and help organisations build and strengthen capabilities, improving their resilience for future emergencies. While many of these practices will already be commonplace, recovery from the current emergency provides an opportunity to reflect and assess against these six practices with more detailed considerations in the report.

Resilience-by-design: improving preparedness of organisations, processes, and facilities

Resilience is required across physical, digital and social systems to anticipate, resist, absorb, recover, and adapt to shocks and stresses. This can be provided in many ways including flexibility and redundancy that can be implemented in design, infrastructure, organisations, training, procurement, regulation, and standards. This investment needs to be made early, embedding resilience from the start and ensuring it is maintained throughout the lifecycle. Resilience should be complementary to other goals such as improving care or decarbonisation. Responsibility for ownership of resilience needs to be clarified at every level.

Responsibility: ensuring clarity of ownership at every level to implement mitigations

Preparing and responding to emergencies requires actions from government at all levels, businesses and the public. Clarity over the leadership and ownership of preparations and implementing mitigation measures is crucial to effective response.

Risk ownership is defined in existing planning frameworks. However, with many risks often overlapping across the remits of multiple government departments, there are examples in the case studies where lack of clarity in ownership hindered the response. During the WannaCry ransomware attack, the role and responsibility of some organisations was initially unclear. The floods in Lancaster raised the importance of ensuring local populations and businesses are aware of flood risks, contingency plans and the provisions of utilities in place to ensure they can best prepare at their individual level.

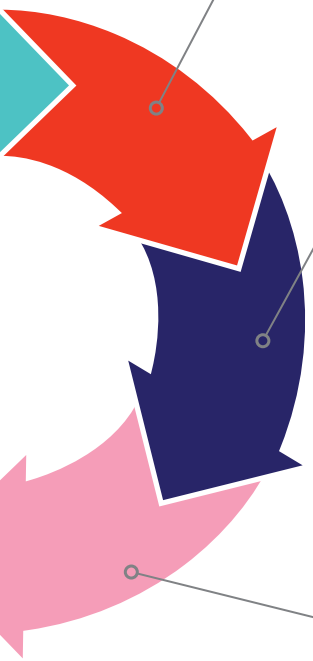
As new organisations are established and old organisations evolve, ownership and accountability should be tested early and regularly to establish roles, improve preparedness, and upskill or increase capacity to ensure that the people who underpin emergency preparedness and response are equipped to do so.

Exercise: practising to build relationships, identify responsibilities and consequences and actions to improve preparedness

Exercises are a crucial tool in emergency preparedness, they enable stress testing of different capabilities and help to improve emergency response. This recommendation, like others, should be seen in the light of advice about drawing sufficiently wide system boundaries: government and local authorities should deploy exercises as broadly as possible to practise their emergency responses but more importantly to build understanding, experience and relationships beyond the resilience teams and across the private sector.

Exercises will expose weaknesses and interdependencies across the response as people involved act to secure their part of the system. Where these vulnerabilities arise, actions to improve resilience should be identified with clear attribution of ownership and responsibility. Real emergencies create further opportunities to learn lessons, the insights they provide should be shared and considered in other contexts. It is vital to take the time to have an open conversation about the challenges faced and adapt accordingly. Fukushima led to change in the nuclear industry and ENWL has installed stilts to mitigate flood risk. However, lessons should not come at the expense of acknowledging that no emergency is the same.

We are calling upon organisational leaders in the public, private and third sector to reflect upon the extent to which these practices for preparedness are incorporated in their business continuity plans or emergency response planning. All organisations need to consider where their interdependencies lie within the wider system, how vulnerabilities can be reduced and resilience strengthened. We are also calling upon individuals and organisations to raise questions, and test policies and decisions against these practices for preparedness to ensure resilience isn't considered as an after-thought by decision-makers and responsibility for resilience is clear across organisations.



Agility: keeping pace with increasing interconnectedness and evolving threats and hazards

Despite stakeholders having learnt and adapted following the events, there was no consensus about being overall better prepared when we examined the case studies. The world is constantly evolving, whether it is the increasing digitalisation and electrification, how we receive information, or the evolution of hazards due to climate change or increasingly sophisticated cyber-attacks. No emergency is ever the same, it is dynamic in nature, and the vulnerabilities and threats continue to change. A forward-looking approach should be built into any approach to preparedness, where these evolving physical, digital and societal contexts can be better understood and the level of ongoing adaption can match the pace of change.

Understanding: mapping of critical capabilities, what they can provide and identification of gaps

Risk planning establishes which government departments lead on the emergency response, but they continue to rely on wider capabilities to be able to respond on the ground. Preparedness requires building an awareness of those capabilities, across the public and private sector, which may be directly required in an emergency response but also those capabilities that can be repurposed to meet demands that were not considered likely. This will strengthen the ability to rapidly mobilise in a response and identify where there might be gaps. Establishing this as part of the planning process enables strategic investment in flexible, agile capabilities across national assets, research and innovation, skills and labour, industrial capability, resources, and the connecting networks.

Organisations will also benefit from clarity of how they may be able to support in an emergency and awareness of their interdependencies within a wider system, for example supply chains or critical infrastructures.

Relationships: building a network of networks across local, national and international boundaries

Across the case studies, the relationships already in place at the time of emergency formed an essential part of the initial fast-paced response. Existing relationships between people and organisations provide an understanding of the knowledge, experience, resources, and skills within an organisation. It is crucial to ensure that a breadth and diversity of trusted relationships and information flows are established and maintained, between those organisations with the required capabilities. Structures such as joint-agency modelling, LRFs, industry-sector bodies, and national and international research collaborations and across the public–private sector interface already support this.

For the relationships and connections established in an emergency response, consideration should be given to knowledge management, for example how those connections are recorded, and whether the relationship is sustained and managed, or actively closed down to understand what connections can be deployed in an emergency.

Recommendations for government

Emergency response at scale requires effective engagement and coordination of capabilities across the public, private and third sector. This can be challenging to incorporate into all current emergency preparedness processes. The case studies **highlighted instances where the systems' boundary didn't go wide enough to consider all of the relevant stakeholders or the interconnections within weren't strong enough or leveraged effectively at the onset of the emergency**.
Applying a wider systems-based view and building a consideration of critical capabilities would guide and shape the implementation of the practices for preparedness with the following:

- A structured identification of the breadth of critical capabilities across the public, private and third sector and the flexible role they play that can enable emergency response to both mitigate risks and seize opportunities.
- An understanding of the interdependencies that exist across risks and response to mitigate concurrent and compound risks with potential for cascade failure, where multiple elements happening at one time trigger an emergency or an initial failure initiates a cascade of failures across an interconnected system.
- The determination of the critical networks and coordination capability for emergency response to ensure they can be involved and strengthened in planning.
- Wider engagement with and from the private sector to leverage their capabilities such as agile manufacturing capability, skills and expertise, and international connections for faster and more effective responses.

This report calls for practical action to build systems thinking and consideration of capabilities deeply into our approach to preparedness enabling adaptability and agility with the implementation of the Integrated Review including the development of the national resilience strategy 2021. Whatever practices and procedures are in place, they risk missing the mark if this is not in place. While this will require upfront investment to strengthen existing capabilities and remedy gaps, immediate and long-term benefits can be delivered through improved emergency response and national resilience. Investment in our existing capabilities goes beyond just provision of insurance for future emergencies, it can deliver wider benefit to the country and society.

The Integrated Review calls for a whole-of-society approach to resilience, so that individuals, businesses, and organisations all play a part in building resilience across the UK. To support this ambition, we are calling on government to partner with the engineering profession and others:

1. **Government should embed a systems approach in emergency planning and preparedness, looking across the public and private sector stakeholders**.
    - Training in systems approaches should be provided to resilience teams across Whitehall and more broadly embedded into the Civil Service to support government decision-making and the implementation of systems thinking within resilience planning.
    - Diversity of experience and expertise should be an active consideration when planning for emergencies and resilience, as a wider range of perspectives will enable better understanding of potential impacts on marginalised and vulnerable groups and stimulate the introduction of new and innovative ways of tackling complex challenges.

2. **Government should undertake an audit to map existing public, private and third sector capabilities and convening bodies against the critical capability groups. This will help build a better understanding of how these organisations and their capabilities can be best deployed to support future emergency response. The audit should be led by the Cabinet Office Civil Contingencies Secretariat (CCS), in partnership with Government Office for Science (GO-Science), devolved administrations and departmental resilience teams responsible for the risks in the National Risk Register (NRR). An aim of the audit should include developing a reporting framework to engage the private sector and build a practical mechanism to keep the audit as live as possible**.
   The audit should inform the following areas:
   - Strategic workforce planning and the skills and training pipeline for resilience in both the public and private sector.
   - Investment in resilience, including clarity of ownership and roles in the Civil Service, public sector research establishments (PSREs), regulators and coordination to leverage industry investment in resilience.
   - Mapping of the national and international networks that already exist, gaps and crucial point contacts.

3. **The CCS, in partnership with GO-Science, should work with the Royal Academy of Engineering and others to develop the critical capabilities approach into a practical tool for emergency planning, preparedness and resilience that builds on existing capabilities programmes. This should include embedding the practices for preparedness alongside current foresight and horizon scanning methods and exercises. This will identify and ensure the right capabilities are in place to respond effectively and with agility to future scenarios and risks**.
   - Risk owners in government should increase the extent and realism of exercises carried out, drawing on the wider capabilities identified in the audit to support the proactive building of networks ahead of time. This should consider participation, frequency, scenario characteristics (scale, location, severity), how much warning is provided and the mechanisms for activating emergency measures. Outcomes should be shared with teams or organisations responsible for mitigation strategies, and regular reviews should be put in place to monitor implementation of lessons.
   - This recommendation directly supports government's priority actions outlined in the Integrated Review to improve our ability to test and develop our capabilities through contingency planning and regular exercises, bringing together government, the emergency services, the armed forces, other local responders and industry. It can support the national resilience strategy work that is already underway.

We are calling for practical action to build systems thinking and consideration of capabilities deeply into our approach to preparedness enabling adaptability and agility with the implementation of the integrated review

Annex A
Case studies

The UK's responses in these case studies are presented as high-level summaries over the subsequent pages. These summaries are not intended to be fully comprehensive as formal reviews have already been undertaken.

Many of the key stakeholders were represented in workshops run by the Academy to explore the case studies in more detail for the purposes of this report.

The illustrated evidence tables produced through the workshops are available through the online version of this report at: raeng.org.uk/policy-and-resources/engineering-policy/security-and-resilience/critical-capabilities.

The Eyjafjallajökull eruption (2010)

On 20 March 2010, the Icelandic volcano Eyjafjallajökull began an initial eruption, followed by a second eruption starting on 14 April. From 15 to 20 April, ash from the volcanic eruption covered large areas of Northern Europe, resulting in countries closing their airspace. 104,000 flights were cancelled during an eight-day period, 48% of total air traffic, affecting millions of passengers globally[53,54,55]. Volcanic activity and ash advisories for areas of ash affecting flights continued to be issued until 23 May 2010.

In the UK, the presence of ash led the **National Air Traffic Services (NATS)** to close UK airspace[56]. The internationally agreed regulation stated that if ash was visible, it was not deemed safe to fly. The **Civil Aviation Authority (CAA)** took the lead in convening experts across the world to define safe and quantified levels of ash concentration for flight and areas where ash concentration was sufficiently low[57,58]. This included bringing together international regulators, aerospace manufacturing companies, operators, and air traffic management.

The **Met Office**, one of nine Volcanic Ash Advisory Centres (VAAC), provided forecasts four times a day on the location of the ash cloud[59,60]. This included gathering inputs for the NAME model, including data from research planes and satellites, and evolved into forecasts of ash concentration and corresponding safe flight zones. There was little available data from nearby the volcano and the research plane was initially unavailable due to maintenance. Collaborations with UK researchers, Icelandic and European counterparts were essential, especially with regards to data collection and analysis.

SAGE was activated with an initial call on 20 April 2010 and had its first meeting on 21 April 2020[61,62]. It brought together expertise to assess the risk of eruption of a second neighbouring volcano, examine the risk to UK health and food, and validated the direction of work of the CAA. Prior to SAGE activation, the Government Chief Scientific Advisor (GCSA) provided updates to the Cabinet Office, CCS and Number 10. This emergency was one of the first SAGE activations. Ownership of the response lay with the CAA and international regulators, the role of government was therefore unclear beyond assessing risk to the UK population.

The **FCO** led on the repatriation of British people stranded abroad[63]. Companies activated their business continuity plans to manage changes in demand in the transport sector, unexpected staff absences and the risk of disruption to supply chains.

Key stakeholders: CAA, SAGE, Rolls-Royce and other aircraft engine manufacturers, airlines including British Airways, European and American aviation regulators and agencies, the Met Office and international counterparts, DfT, British Geological Survey (BGS), volcanologists.

The response to the emergency faced a number of challenges:

- **NRR** – ash cloud was not included in the NRR and the UK government had not prepared for such an event ahead of time.
- **Regulation** – the international regulation defined safe flight based on an absolute: visibility of ash or no ash. There was little evidence available on the effects of ash density, ash characteristics and flight time on aircraft engines.
- **Defining the scientific question** – SAGE was initially tasked with questions related to health and agriculture. It took time to reach the question on flight regulation, by which point the emergency was almost over.
- **Modelling** – little data was available from a close proximity to the volcano to input into the Met Office model increasing uncertainty. The research plane was under maintenance causing delay to the response. Satellite data was available but this was mainly qualitative, providing information on presence of ash rather than concentration. The requested output from the Met Office model changed during the emergency from location of the ash cloud to location and density of the ash cloud.

Timescale: **7 days**
20 March 2010: **Eruption start (small)**
14 April 2010: **Second eruption begins**
15–20 April 2010: **Airspace closed**
May 2010: **Local airspace disruption**
October 2010: **Eruption officially over**

- **Challenging communications** – airlines disputed the regulator's interpretation of the rules and decision to close airspace. There was no prior warning or discussion with industry ahead of the NATS decision.
- **Geographical vulnerabilities** – European airspace has a very high density, compounding impact due to the difficulty of re-routing flights compared to other parts of the world.

Key learnings:

- **Considering resilience in regulation** – understanding where there are gaps in knowledge and potential risks from regulation ahead of time would improve clarity in communication and allow to fill these gaps for better preparedness[64].
- **Official structures and responsibilities** – the Met Office was one of nine World Meteorological Office VAACs that operated for the benefit of aviation under International Civil Aviation Organisation (ICAO) rules. It was not set up to consider questions related to food and environment, which were of interest to the government. Government did not have a well-defined role in the mitigation of impact on the aviation sector, which was led by the CAA[65].
- **Bringing together the source data/modelling/output chain** – the Met Office's NAME model was key to forecasting the location of the ash cloud. Challenges arose in terms of source data and changing output requests. The ability to rapidly collect source data and then produce well-defined outputs is crucial to the delivery of an effective response. International research collaborations had an important role to input into the data chain. The Met Office at the time was not set up to respond to questions beyond ash for aviation.
- **Industry expertise into government and composition of SAGE** – initial questions for SAGE did not include the consideration of the impact on flight safety, nor was aerospace engineering expertise directly included. This was in part due to the ownership of the response lying with the regulator. Rolls-Royce found its own route to contact the GCSA. Industry expertise was also fed into SAGE via the DfT.
- **International research collaboration and expertise** – the Met Office and UK-based volcanology research groups had existing collaborations with Icelandic researchers, which facilitated part of the response. One UK researcher with expertise on the specific volcano was found and provided information to SAGE. National and international collaborations, including R&D related to volcanic ash, have continued since.

Are we better prepared now?

The CAA, working with international regulators and aviation bodies, developed and implemented an updated regulatory regime which was used during the 2011 Grimsvotn volcano eruption[66]. A major exercise was run across Europe involving the European Aviation Safety Agency, regulators, air traffic controllers, operators, and airlines. A single Volcanic Ash Contingency Plan is now in place for both the ICAO North Atlantic Region and European Region to provide contiguous response. Rolls-Royce has tested and certified their engines for a range of ash concentrations, equivalent to approximately 10% of the global fleet. This is not the case for all engine manufacturers and could lead to flights being grounded in another volcanic ash event.

Risk from volcanic eruptions is now included in the NRR and investment has been made into modelling and observational capability. The Met Office, Icelandic Met Office, BGS and National Centre for Atmospheric Science have signed a Memorandum of Understanding and continue to collaborate. Additional investment has been made in the NAME model and satellite processing, and the UK has developed an operational LIDAR capability. Since 2010, considerable international and national research and collaboration continues to take place in areas including volcanology, atmospheric modelling, and detection and impacts of volcanic ash and gases.

Other concerns raised during the workshop included the risk of sulphur emissions in a future eruption, with potential impacts on public health and agriculture, and assessing the risks to flights with increasing extreme weather caused by climate change.

The UK response to the Fukushima nuclear accident (2011)

On 11 March 2011, a severe nuclear accident happened at the Fukushima Daiichi Nuclear Power Plant in Japan. An earthquake-triggered tsunami flooded the power plant's lower grounds damaging the emergency generators which the plant was relying on to power the pumps circulating coolant. The loss of coolant led to three nuclear meltdowns, three hydrogen explosions and the release of radioactive contamination.

Following the explosion at Tokyo Electric Power Company's (TEPCO) Fukushima Daiichi nuclear power plant, a **COBR** meeting activated **SAGE** to compile, peer review, and interpret scientific information relevant to the evolving situation[67,68]. The **Met Office** led joint agency modelling efforts to understand the risks due to potential radioactive releases and the weather and predict the wider impacts. International networks and connections were used to gather information about the TEPCO plant and to verify UK analysis.

SAGE developed a reasonable worst-case scenario that informed policy decisions to ensure the safety of 170,000 UK citizens living in Japan at the time of the Fukushima nuclear disaster. Through the **British Embassy**, support was provided to UK citizens in Japan. Given the rate of information disseminated by the Japanese government, the trusted UK analysis was also being used by Japanese citizens.

Staff at the British Embassy in Tokyo, which was not affected by the earthquake, were mobilised to form a crisis response centre to guide relief efforts[69]. The embassy team also provided consular assistance to displaced UK citizens who were directly affected, and it constantly monitored information in the media and from the Japanese government to brief colleagues in London.

Key stakeholders: SAGE, GO-Science, FCO, Met Office, Public Health England, Office for Nuclear Regulation, Sellafield Ltd, MoD, Japanese government, British Embassy in Japan, National Nuclear Laboratory, Japan's Nuclear Regulation Authority, International Atomic Energy Agency, US and German Chief Scientific Advisors, French nuclear authority

The response to the emergency faced several challenges:

- **Compound risks to manage** – the Fukushima disaster resulted from a tsunami that caused flooding, followed by an earthquake and landslide that caused a power loss, causing reactors to explode putting others at risk and concerns that ponds for storing fuel risked overheating. These compound factors increase the uncertainty when trying to understand the cause.
- **Tendency to fight the last emergency** – with Fukushima, it was important to dispel the similarities with Chernobyl in order to assess the situation as a unique one. No two events will be the same.
- **Desire to influence** – the SAGE group was small but there were many organisations outside of SAGE feeding in information. While this information was useful many people vying for influence can be difficult to manage.
- **Quantifying uncertainty** – sensibly compiling all the assumptions and unknowns while avoiding information overload is a challenge.

Key learnings

- **International collaboration** – access to international networks was a vital information source and verification mechanism for scientific analysis.
- **Role for close relationships** – UK agencies and academics have seen and continue to see increased links, collaboration and better communications.

- **Dual time frame** – there is inherent uncertainty in emergencies, especially early on. There is value in having initial rough estimates that are validated with care over a longer period as more information becomes available. This second slower-paced response can complement the initial necessarily fast-paced response, including any important corrections.
- **Value in a trusted information source** – the UK Government Chief Scientific Adviser briefings proved popular with UK and Japanese citizens and were seen to be credible.

Are we better prepared now?

Formalisation of the Joint Agency Modelling Partnership is now a vital part of UK formal response structure to radiological accidents. This includes operators, regulators, Met Office, Public Health England, Environment Agency, Food Standards Agency, and the Department for Business Energy and Industrial Strategy and has included work on source data, modelling, impacts, and communications. Ongoing development of this capability during peacetime would facilitate more effective deployment in an emergency.

European collaboration and links have been enhanced through Horizon 2020 projects and direct research collaborations. Ongoing UN activities under the International Atomic Energy Agency and United Nations Scientific Committee on the Effects of Atomic Radiation. As well as addressing specific challenges, these activities also continue to support links and relationships.

As a result of the cascading failure observed at Fukushima, the UK nuclear industry has invested in improvements to safety cases to ensure sites adequately demonstrate the capability for dealing with concurrent events and that there is a breadth of stakeholder oversight[70]. However, recent radiological events have helped to highlight the variety of different risks indicating that ongoing research and innovation and flexibility are needed.

Timescale: **8 days**

11 March: **Earthquake strikes and major Tsunami causes serious damage at Tokyo Electric Power Company (TEPCO) Fukushima Daiichi nuclear power plant**

12 March: **Radiation levels in No.1 reactor reported to rise and hydrogen explosion at reactor No.3**

13 March: **Chief Cabinet Secretary Yuko Endo warns of further explosions**

14 March: **2nd Hydrogen explosion at reactor No.3**

15 March: **US Navy repositions ships and plans**

16 March: **Fires at No.4 reactor**

17 March: **Japanese Self-Defense Forces dump seawater on No.3 and No.4**

19 March: **Japan's National Police Agency lead search for survivors**

Lancaster floods with loss of electricity (2015)

On 5 December 2015, flooding from Storm Desmond led to the loss of electricity supply to 61,000 properties in Lancaster[71,72]. The situation returned to normal by 11 December.

ENWL led the response to restore power, including bringing in 75 large diesel generators from across the country to restore supply. A second fault created additional delays in restoring electricity after the initial flooding was addressed.

Loss of electricity resulted in loss of communications, including wireless home phones, mobile phone and mobile internet signal. **Local radio** provided updates, as well as signs outside schools and word of mouth. The **local council** was able to access the emergency communications system of the LRF.

The **hospital** had back-up generators and fuel for 14 days, but A&E also became the first port of call when access was lost to 111, GPs and pharmacies. The hospital also became the go-to place for queries, effectively acting as a community centre. Other care facilities such as nursing homes did not have back-up generators. **Schools** closed and were faced with the challenge of communicating the decision to parents.

Retail was disrupted, especially an inability to accept card payments. Only some ATMs still worked. Sunday trading hours limited supply despite high demand. The local council had to organise additional waste collection to account for perished goods normally kept in fridges and freezers.

Rail travel was disrupted by the lack of lighting. Buses relocated to an alternative stopping point as the bus station was flooded and refuelled with hand pumps. Provision of other utilities was unaffected, although in modern blocks of flats, water and sewage was disrupted by their reliance on electricity.

Key stakeholders: ENWL, Lancaster City Council, police, fire service, Bay radio, the hospital, schools, university, care providers, residents

The response to the emergency faced several challenges:

- **Loss of communication** – informing residents of decisions or actions to take during the emergency was challenging and, in many cases, the response was coordinated with the support of people living outside the affected zone and able to receive information and communicate.
- **Outside decision-making power with local impact** – the responsibility for the regulation causing the train station to close because of the lack of lighting and shops to close because of Sunday trading rules lie outside of Lancaster, removing flexibility to respond to elements of the emergency.
- **Identifying and supporting vulnerable people** – nursing home residents, elderly people or those living in high rises were disproportionately affected and, without communication, challenging to locate.

Key learnings

- **Diversity and disparate impact on different populations** – beyond the immediate technical response to the flood and electricity loss, a corresponding care and support response may be needed, in some cases with unexpectedly vulnerable groups. This requires a different set of skills and planning. For example, the hospital was well prepared with back-up generators, whereas the care homes did not have back-up electricity and one relied on a camper van to serve warm drinks.
- **Limited resources** – nearly all the readily available large generators in the country were deployed in Lancaster. Concurrent flooding and loss of electricity elsewhere would have cause significant strain on those resources. Similarly managing a similar event with higher impact, for example a larger city with more high rises, would be challenging.

- **Considering loss of communications in planning** – with loss of communication during an emergency, communication prior to the event to ensure the population is aware of good practices is just as important, as well as contingency planning for those organisations involved in the emergency response. For example, using a radio as a source of information may not be instinctive to younger generations, or available to them without forward planning.
- **Responsibility for individual resilience** – campers were found to be resilient, equipped with gas stoves, torches and experience of living without electricity. Even in those areas where flooding is relatively frequent, it can be challenging to ensure the population are well prepared.
- **Levels of service** – regulated infrastructure has to maintain a certain level of service. However, residents and businesses may not be aware of its resilience or plan for loss of service. It can be challenging to make the case for the cost of resilience to regulators.
- **Privatisation and contracting of public services** – this has reduced the central coordination and working relationships between organisations.
- **Information vacuum and misinformation** – rumours circulate very quickly, even when communications are lost. The hospital in effect became a community hub, with people coming to seek information and electricity. This new role was not necessarily accounted for in emergency planning and as such placed a strain on the contingency measures in place to keep it running as a critical service.

Are we better prepared now?

ENWL has put the transformer on three-metre-high stilts, mitigating for the risk of damage from flooding. However, the impact of loss of electricity and communications was viewed to likely be worse now because of an increased dependence on mobile phones, internet and electricity.

Timescale: **7 days**

5 December: **Met office issued a red severe weather warning for rain in Cumbria and North Lancashire**

10:45pm 5 December 2015: **Loss of electricity supply to 61,000 homes**

4:30am Monday 7 December 2015: **Electricity progressively restored**

4pm Monday 7 December 2015: **Loss of electricity. Diesel generators brought into the city and power restored over next few days**

Friday 11 December: **Situation back to normal**

Cities are a dynamic system bringing together old and new interdependent elements. As electrification increases, including cars and doors for example, and climate change increases the likelihood of flooding in the UK, new vulnerabilities in a power loss event will need to be mitigated. Uptake of electric cars may introduce challenges both during the emergency, with the inability to charge or use the car radio for information, and when the local grid is restarted.

Similarly increasing reliance on mobile phones introduces the risk of wider loss of communications, with decreasing numbers of public phones and landlines[73]. Social media has also introduced quicker spread of both information and misinformation, although limited in the populations they reach. Emergency responders are developing methods to best manage communications and avoid creating an information vacuum for misinformation to spread.

The WannaCry ransomware attack (2017)

On 12 May 2017, a global ransomware attack, known as WannaCry, affected more than 230,000 computers in at least 150 countries. Although not directly aimed at the NHS, 34 trusts were infected and 46 were affected resulting in 30,500 cancelled appointments and 595 GP services impacted. None of the affected organisations had applied the Microsoft update patch advised by NHS Digital on 25 April 2017, following intelligence of a specific threat from BT. The incident lasted a week until 19 May 2017. Five acute trusts were diverting patients from their A&E departments and several trusts were experiencing issues with diagnostic services leading to cancelled appointments and procedures[74].

The response started when **GCHQ** and **NCSC** were alerted to the untargeted proliferation of WannaCry ransomware across the world. It took a few hours before information started to gather on the impact on the NHS, which initiated the UK's first ministerial **COBR** meeting following a cyber-attack.

A cross-departmental emergency team was mobilised and lead by **NHS England** with a focus on collecting data and ensuring patient safety and continuity of care. Technical skills were deployed from **NHS Digital**, **NHS trusts**, suppliers, and manufacturers to patch the systems and disable the ransomware and the 'kill switch' was identified by an interested researcher[75].

The disruption was communicated through the BBC to inform the public and NHS networks to keep trusts updated. To reduce the impact of the attack beyond the NHS, guidance was communicated to industry through the Cyber Security Information Sharing Partnership, a joint industry and government initiative set up to exchange cyber threat information.

The National Crime Agency centre worked with UK and international partners to share intelligence and coordinate action against responsible actors[76].

Key Stakeholders: NHS England/Improvement, NHS Digital, Department of Health and Social Care, NCSC, National Crime Agency, healthcare trusts, IT delivery partners, manufacturers, and commissioning support units.

The response to the emergency faced several challenges:

- **Disruption to care** – unable to access electronic patient records and clinical systems, and some medical equipment was taken out of service so patients had to be diverted to other trusts.
- **Lack of clear problem owner** – the recent formation of the NCSC meant a cyber event had not been extensively exercised and clear roles and responsibilities had not been assigned. The role for NHS Improvement was initially unclear as they were not explicitly listed in the EPRR legislation. The range of organisations involved caused confusion at the local level as NHS organisations reported the WannaCry attack to different national bodies.
- **Communication** – communication between central government organisations and trusts complicated the response. It was challenging to gather information on the extent of NHS trusts that were infected or affected, central guidance on what to do was lacking and unhelpful messaging on the Cyber Security Information Sharing Partnership (CiSP) caused confusion. In the worst cases, some trusts shut down their networks, closing down email access with no alternative communication methods in place. There was a reluctance to communicate the incident to the press because of wider concerns about the implications for trust in digital healthcare, which to some extent was prohibitive to the response.
- **Skills shortages** – NHS Digital and NCSC only had cybersecurity staff to manage the central systems so patching the complex distributed systems within hospitals and across trusts required mobilisation of the trusts' IT professionals, which are a scare resource. To support these efforts, external suppliers, consultants offering help and equipment

manufacturers were enlisted but managing these offers of help was challenging.

Key learnings

- **Practice helps** – the parts of the response that organisations exercise and deploy regularly were delivered well in a wider incident. Examples from WannaCry included NHS trusts diverting services or NCSC identifying technical solutions. Across the NHS where structures are continuously evolving, regular exercises with the relevant organisations are vital to ensure clarity on accountability. Unplanned exercises help identify the capabilities that exist with a skeleton staff.
- **Distributed attack** – the central NHS bodies and the Department of Health and Social Care considered themselves relatively prepared for a severe attack, but there was a disconnect between central organisations and the people responding on ground and managing the consequences. There is a large disparity in digital capability across hospitals depending on skills and infrastructure.
- **Assessment of risk** – many trusts had failed to identify cybersecurity as a risk to patients or care outcomes and trusts tended to overestimate their ability to respond to cyber incidents. Security is generally viewed as an add-on, especially when competing with funding for care services and lack of a clear enforcement body for cybersecurity actions. Resilience of healthcare service provision to different types of risks needs to be considered.
- **Communication of risk** – communicating the risk in terms of patient harm and disruption to delivery of services is anecdotally more effective that talking about cybersecurity risks. Upskilling boards and audit committees in how to question these risks has been an important intervention.

Are we better prepared now?

Since WannaCry, NHS Digital has worked to improve communication and recognition of the importance of patching systems, which means disruptions due to negligence are less likely. Microsoft Advanced Threat Protection (ATP) has been centrally procured by NHS Digital to give local organisations, such as hospitals and GP surgeries, better cybersecurity protection.

Timescale: **7 days**

17 March and 28 April: **Asked to patch system**

Morning of 12 May: **First problems reported**

1pm 12 May: **NHS England EPRR notified**

4pm 12 May: **Major incident declared, COBR meeting putting NHS England in charge**

Evening of 12 May: **Researcher activated a 'kill-switch'**

12–15 May: **Secure emergency care pathways**

15–19 May: **Patch rest of systems**

19 May: **Incident stood down**

Roles and responsibilities have been better defined in the event of another major cyber-attack, and a central coordination centre has been established. However, further structural changes mean this won't remain static. CareCERT has created a system platform to help manage the demand, including back-up with instant response companies to provide advice remotely. A cyber associates network has been set up to improve the consistency of communication across prevention, advice and guidance, and feedback mechanisms on whether action has been taken have been improved.

However, cyber-attacks are getting more sophisticated, and a targeted malicious attack will still pose challenges. Trends of increasing digitalisation of NHS services, greater connection between primary, secondary and social care settings, and increasing privatisation of services introduces greater network complexity and vulnerabilities if security standards are not clearly articulated and implemented. There was a feeling at the workshop discussion that cybersecurity was still undervalued within NHS trusts, but improvements were being made, including a change in the communication approach presenting risk in terms of patient harm, training for boards and upskilling audit and risk committees to understand the necessary cybersecurity challenges. Wannacry showed that in such a broad and complex network, the system is only as secure as its weakest link.

Annex B
Working Group

Chair

Paul Taylor FREng
Director, Morgan Stanley International

Sir John Beddington CMG HonFReng FRS FRSE
previously Government Chief Science Adviser

Lianne Deeming FREng
Chief Executive Officer, BlueLight Commercial

Professor Anthony Finkelstein CBE FREng
Chief Scientific Adviser for National Security

Professor David Gann CBE
Pro-Vice Chancellor for Development and External Affairs, University of Oxford

Dame Judith Hackitt DBE FREng
Chair of Make UK

Professor Nick Jennings CB FREng
Vice-Provost (Research and Enterprise), Imperial College London

Professor Dame Angela McLean DBE FRS
Chief Scientific Adviser, Ministry of Defence

Professor Tim Palmer CBE FRS
Royal Society Research Professor in Climate Physics, University of Oxford

Dr Fiona Rayment OBE FREng
Chief Science and Technology Officer, National Nuclear Laboratory

Catriona Schmolke FREng
Previously Senior Vice-President, Jacobs

Auriol Stevens, Global IT Director
Applied Technology, Unilever

Professor Eleanor Stride FREng
Professor of Engineering Science, University of Oxford

Rear Admiral John Trewby CB FREng
previously chair University Hospital Southampton Foundation Trust and Harris Defence Ltd

Academy staff

Dr Shabana Haque OBE, Head of Engineering Policy
Dr Marie-Laure Hicks, Policy Advisor
Dr Corina Shika Kwami, Policy Advisor
Dr Alexandra Smyth, Senior Policy Advisor
Dr Nick Starkey, Director of Policy

Annex C
Contributors

A range of stakeholders were involved over the course of this project. Individuals from the following organisations at the time of or shortly after the emergencies investigated were consulted to build our case studies.

- Cabinet Office Civil Contingencies Secretariat
- Cranfield University
- Department for Transport
- Electricity North West
- Government Office for Science
- Environment Agency
- Imperial College London
- Jacobs
- Lancaster City Council
- Met Office
- Ministry of Defence
- NHS Digital
- NHS England/Improvement
- NHSX
- National Cyber Security Centre
- National Nuclear Laboratory
- National Physical Laboratory
- Rolls-Royce
- Royal Society
- Sellafield
- University College London
- University of Cambridge
- University of Lancaster

References

1 Supply chain challenges, lessons learned and opportunities, National Engineering Policy Centre, July 2020
2 Innovation in a crisis: webinar series, Royal Academy of Engineering, 2020 [Accessed 06/01/2021]
3 Innovation in a crisis: webinar series, Royal Academy of Engineering, 2020 [Accessed 06/01/2021]
4 *Statement of Ethical Principles*, Royal Academy of Engineering and Engineering Council, 2017
5 *Thinking like an engineer*, Royal Academy of Engineering, 2014
6 Preparation and planning for emergencies, Cabinet Office, 20 February 2013
7 Dealing with civil contingencies: emergency planning in the UK, House of Commons Library, 11 July 2017
8 Coronavirus Act 2020
9 National Risk Register, HM Government, 2020
10 Evaluating UK natural hazards: the national risk assessment, Parliamentary Office of Science and Technology, 24 April 2019
11 Preparation and planning for emergencies, Cabinet Office, 20 February 2013
12 Responding to Emergencies: the UK Central Government Response, Cabinet Office, 19 April 2013
13 National Risk Register, HM Government, 2020
14 About SAGE. [accessed 15/09/2020]
15 Interview notes
16 COBR Explainer, Institute for Government. [Accessed 07/12/2020]
17 Dealing with civil contingencies: emergency planning in the UK, House of Commons Library, 11 July 2017
18 Emergencies: preparation, response and recovery: Local resilience forums, Cabinet Office, 20 February 2013
19 Interview notes
20 Defence in Depth in Nuclear Safety, International Atomic Energy Agency, 1996
21 Evaluating UK natural hazards: the national risk assessment, Parliamentary Office of Science and Technology, 24 April 2019
22 Interdependency: physical, digital, geographic or organisational links that enable transfer or sharing of risk, failure or mitigation
23 Impact of volcanic ash on air traffic, EUROCONTROL, 01/07/2010 [accessed 15/09/2020]
24 Volcanic Ash: societal and economic damage from volcanic ash clouds reduced as a consequence of Bristol research, REF2014 impact case studies [accessed 04/01/2021]
25 Ash-cloud of April and May 2010: impact on air traffic, ICAO Paris [accessed 04/01/2021]
26 Living without electricity, Royal Academy of Engineering, 2016
27 Reflections on the Lancaster power cuts of December 2015, DEMAND, 20 January 2016 [Accessed 06/01/2021]
28 The challenges of cybersecurity in health care: the UK National Health Service as a case study, Saira Ghafur et al. 2019
29 Impact of volcanic ash on air traffic, EUROCONTROL, 01/07/2010 [accessed 15/09/2020]
30 Volcanic Ash: societal and economic damage from volcanic ash clouds reduced as a consequence of Bristol research, REF2014 impact case studies. [accessed 04/01/2021]
31 Ash-cloud of April and May 2010: impact on air traffic, ICAO Paris. [accessed 04/01/2021]
32 Living without electricity, Royal Academy of Engineering, 2016
33 Reflections on the Lancaster power cuts of December 2015, DEMAND, 20 January 2016. [Accessed 06/01/2021]
34 The challenges of cybersecurity in health care: the UK National Health Service as a case study, Saira Ghafur et al. 2019
35 VentilatorChallengeUK. [accessed 16/12/2020]
36 Life saving breathing aid developed to keep COVID-19 patients out of intensive case, NIHR, 30 March 2020. [Accessed 06/01/2021]
37 UCL Ventura breathing aids for COVID-19 patients, UCL. [Accessed 06/04/2021]
38 Coronavirus (COVID-19): scaling up our testing programmes, DHSC, 6 April 2020
39 Testing, gov.uk [accessed 1/03/2020]
40 NHS Test and Trace statistics (England): methodology, DHSC, 10 December 2020
41 The government's approach to test and trace in England – interim report, National Audit Office, 11 December 2020
42 Lessons learnt: the role of academia and industry in the UK's diagnostic testing response to COVID-19, Academy of Medical Sciences, November 2020
43 Precautionary SAGE 1 minutes, GO-Science, May 2020
44 List of participants of SAGE and related sub-groups, Government Office for Science, 4 December 2020
45 Science advice in a crisis, Institute for Government, December 2020
46 The UK response to COVID-19: use of scientific advice, House of Commons Science and Technology Committee, 8 January 2021
47 CEPI to fund three programmes to develop vaccines against the novel coronavirus, nCov-2019, CEPI, 23 January 2020
48 COVAX: ensuring fair allocation of a COVID-19 vaccine, CEPI, 26 June 2020
49 COVAX explained, Gavi, 3 September 2020
50 CEPI establishes global network of laboratories to centralise assessment of COVID-19 vaccine candidates, CEPI, 2 October 2020
51 Coronavirus: 5G and microchip conspiracies around the world, BBC Reality Check, 26 June 2020
52 COVID-19 news and information: consumption and attitudes, Ofcom, 9 April 2020
53 Impact of volcanic ash on air traffic, EUROCONTROL, 01/07/2010 [accessed 15/09/2020]
54 Volcanic Ash: societal and economic damage from volcanic ash clouds reduced as a consequence of Bristol research, REF2014 impact case studies. [accessed 04/01/2021]
55 Ash-cloud of April and May 2010: impact on air traffic, ICAO Paris. [accessed 04/01/2021]
56 Five years on from the Ash Cloud Crisis, what's changed? NATS, 2015. [Accessed on 2 March 2021]
57 A history of ash and aviation, CAA. [accessed 04/01/2021]
58 Volcanic ash and its danger to international civil aviation, ICAO. [accessed 04/01/2021]
59 Memorandum submitted by the Met Office, House of Commons Science and Technology Committee, 16 September 2010. [accessed 04/01/2021]
60 The London VAAC process, Met Office. [accessed 04/01/2021]
61 Scientific advice in emergencies, House of Commons Science and Technology Committee, 14 February 2011
62 The role of science advice in planning and responding to a major UK emergency, National Archives, 5 July 2013. [accessed 04/01/2021]
63 Royal Navy ships to return Britons stranded by volcano, BBC, 19 April 2010
64 Risk, interest groups and the definition of crisis: the case of volcanic ash, B. M. Hutter and S. Lloyd-Bostock, British Journal of Sociology, 64 (3), pp. 383–404, 2013.
65 Memorandum submitted by the Royal Aeronautical Society (SAGE 10), RAeS, 2010.
66 A history of ash and aviation, Civil Aviation Authority. [accessed 15/09/2020]
67 The role of science advice in planning and responding to a major UK emergency, National Archives. [Accessed 07/01/2021]
68 The UK Response to Fukushima and Anglo-Japanese Relations, R. W. Grimes et al, Science & Diplomacy, Vol.3 (2), June 2014
69 The aftermath of the Fukushima Daiichi Accident: a Perspective from the British Embassy in Tokyo, R.J Oppenheim et al, Clinical Oncology 28, 272–274, 2016
70 Fukushima and the UK nuclear industry, ONR. [Accessed 07/01/2020]
71 Living without electricity, Royal Academy of Engineering, 2016.
72 Reflections on the Lancaster power cuts of December 2015, DEMAND, 20 January 2016. [Accessed 06/01/2021]
73 The future of fixed telephone services, Ofcom, February 2019
74 The challenges of cybersecurity in health care: the UK National Health Service as a case study, Saira Ghafur et al. 2019
75 Lessons learned review of the WannaCry Ransomware Cyber Attack, William Smart, February 2018
76 The cyber threat to UK business, National Crime Agency and National Cyber Security, 2017–2018

Royal Academy of Engineering

The Royal Academy of Engineering is harnessing the power of engineering to build a sustainable society and an inclusive economy that works for everyone.

In collaboration with our Fellows and partners, we're growing talent and developing skills for the future, driving innovation and building global partnerships, and influencing policy and engaging the public.

Together we're working to tackle the greatest challenges of our age.

What we do

TALENT & DIVERSITY

We're growing talent by training, supporting, mentoring and funding the most talented and creative researchers, innovators and leaders from across the engineering profession.

We're developing skills for the future by identifying the challenges of an ever-changing world and developing the skills and approaches we need to build a resilient and diverse engineering profession.

INNOVATION

We're driving innovation by investing in some of the country's most creative and exciting engineering ideas and businesses.

We're building global partnerships that bring the world's best engineers from industry, entrepreneurship and academia together to collaborate on creative innovations that address the greatest global challenges of our age.

POLICY & ENGAGEMENT

We're influencing policy through the National Engineering Policy Centre – providing independent expert support to policymakers on issues of importance.

We're engaging the public by opening their eyes to the wonders of engineering and inspiring young people to become the next generation of engineers.

Royal Academy of Engineering
Prince Philip House
3 Carlton House Terrace
London SW1Y 5DG

Tel 020 7766 0600
www.raeng.org.uk
@RAEngNews

Registered charity number 293074

Front cover images: