STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

HOUSE OF LORDS

National Resilience Committee

Report of Session 2026–27

Are we ready? Building a culture of resilience

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026. You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Ordered to be printed 29 October 2026 and published 16 November 2026

Published by the Authority of the House of Lords

HL Paper 79

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

National Resilience Committee

The National Resilience Committee was appointed by the House of Lords "to consider national resilience, including the role of local resilience".

Membership

The Members of the National Resilience Committee were:

Baroness Coussins (Chairman)
Lord Farmer
Baroness Helic
Baroness Hunter of Auchenreoch
Lord Marland
Baroness MacLeod of Camusdarach
Baroness Mobarik
Rt Hon Baroness Northover
Lord Oates
Lord Peach
Baroness Paul of Shepherd's Bush
Rt Hon Lord Spellar

Declaration of interests

See Appendix 1.

A full list of Members' interests can be found in the Register of Lords' Interests: http://www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests

Publications

All publications of the Committee are available at: https://committees.parliament.uk/committee/832/national-resilience-committee/publications/

Parliament Live

Live coverage of debates and public sessions of the Committee's meetings are available at: http://www.parliamentlive.tv

Further information

Further information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is available at: https://www.parliament.uk/business/lords

Committee staff

The staff who worked on this Committee were Rhouda Elalfy (Clerk), Robert Wilson (Policy Analyst) and Mark Gladwell (Committee Operations Officer).

Contact details

All correspondence should be addressed to the National Resilience Committee, Committee Office, House of Lords, London SW1A 0PW. Telephone 020 7219 4621. Email *hlnationalresiliencecom@parliament.uk*

Social media

You can follow the Committee on LinkedIn: National Resilience Committee

Copyright and privilege

This report was published by Order of the House of Lords and is subject to Parliamentary Privilege. Content may be reproduced under the terms of the Open Parliament Licence, which is published at https://www.parliament.uk/copyright. © Parliamentary Copyright House of Lords 2026.

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

CONTENTS

Page

Summary 3

Summary of conclusions and recommendations 6

Chapter 1: Introduction 17
This inquiry 17
Other relevant work and inquiries 18
Government activity 19
Evidence and engagement 21

Chapter 2: Interconnected risks and threats 22
Defining resilience and responsibility 22
What is resilience? 22
What does a whole-of-society approach mean? 22
The changing risk landscape 23
Chronic risks and acute risks 23
Hostile and sub-threshold state activity 23
International instability and supply-chain exposure 24
Box 1: Supply chain vulnerabilities 27
Cross-sector dependencies 28
Plans, strategies and frameworks 29
Long-term preparedness 30

Chapter 3: Governance 32
Risk assessment 32
Data sharing 32
Resilience planning 34
Leadership 35
Government structures 37
Legislation 39
Existing and proposed legislation 39
Future legislation 41
International frameworks 43

Chapter 4: Activating the whole of society 45
Who has a role to play? 45
Vision and plans 46
Box 2: International case studies 47
Delegating Responsibility 48
The Role of the Private Sector 49
Education and Training 52
Exercising and Stress Testing 55
Volunteers and Civil Reservists 57
Box 3: Civil protection initiatives 59
Funding 60
Home defence 61

Chapter 5: Communications and developing a culture of resilience 63
Information environment 63
Disinformation and misinformation 64
Digital communications 66
Individual mindset and public communication 68

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Guidance 70
Collective mindsets 72
Community mindset 72
Box 4: Community good practice 72
Government mindset 73
Appendix 1: List of Members and declarations of interest 75
Appendix 2: List of evidence and committee activity 77
Appendix 3: Call for evidence 88
Appendix 4: National situation centre visit note 90
Appendix 5: Scenario simulation exercise note 91
Appendix 6: University student roundtable summary note 93
Appendix 7: Finland visit summary note 97

Evidence is published online at: https://committees.parliament.uk/committee/832/national-resilience-committee/.

Q in footnotes refers to a question in oral evidence.

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

SUMMARY

The world is more turbulent and insecure than it has been for decades. Yet, in the face of potentially catastrophic risks and despite the recent launch of the Be Ready campaign, the Government appears complacent and the UK is underprepared. We need to move fast to turn things around.

The public don't have a full picture of the level and frequency of current sub-threshold hostility against the UK from Russia, China and Iran in the form of cyber-attacks, proxy acts of violence, or threats to undersea cables and pipelines on which our communications and energy flows depend.

Against these, as well as the possibility of escalation to armed attack, our defence hardly looks resilient, as the Strategic Defence Review and subsequent controversy over the Defence Investment Plan have illustrated. The number of attempted cyber-attacks on the UK's defence system is already over 90,000 a year. The Director of MI5 has said that AI is 'supercharging' risks ranging from cyber-attacks to the development of biological weapons. The Chief of the Defence Staff has said the risks and threats to the UK are "greater than I have known since the Cold War".[1]

Current resilience plans are largely out of date in that they address a possible crisis or emergency in, for example, a power outage or disruption to water supplies, or a cyber-attack, or a biochemical hazard, or collapsing infrastructure, but not the 'polycrisis' of multiple emergencies happening simultaneously or cascading into one another. Systems must come out of their silos and interrelate across Government and society as a whole. They must focus on planning and preparedness, not just response and recovery. Prevention is better–and cheaper–than cure. Supply chains depend on highly interconnected systems. Disruption in one part of the chain can quickly have consequences elsewhere.

The good news is that we aren't starting from scratch. There are dozens of committees, strategies, action plans and frameworks with the word 'resilience' in the title, ranging from the UK Resilience Academy to the Ely Area Resilient Community Group Plan.

The trouble is most of them don't link up with the others, meaning that there is a great deal of overlap and duplication, but not much consistency. What's missing is leadership and inclusive, interconnected systems which link overall strategy to operational capacity on the ground, based on a clear picture of what national, regional, organisational, community, household and individual preparedness and resilience should look like. The private sector must also be embedded in resilience planning and systems; at present, businesses sit on the fringes.

The public say they expect emergencies to become more frequent and are ready to respond positively but have no clear, authoritative information on what they should do to be prepared. The Government's recent announcement of a three-year Be Ready campaign to plug that gap will, we hope, be a constructive start. We believe the Government must go much further and faster in advancing national resilience.

Legislation and regulations also need updating. For example, while digital infrastructure, communications, energy, food and transport are explicitly

1 BBC News, *UK in most dangerous period I've known, military chief says*, 5 June 2026

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

recognised as Critical National Infrastructure, the status of essential medical supplies, including blood, medicines and medical equipment, is less clearly defined within the health sector.

We were shocked to discover that the UK imports 80% of the active ingredient for penicillin antibiotics and a large proportion of all other antibiotics from China and that the UK no longer has any domestic antibiotic manufacturing capacity whatsoever of its own, the last domestic plant having closed down in 2025. Indeed, there remains only one antibiotic manufacturer in the whole of Europe.

Another sobering fact is that just nine retailers account for around 94.5% of food sold through UK supermarkets.

Interruption to the supply chains of food, medicines and a wide range of other items and services is at the heart of what an up-to-date national resilience system needs to tackle, shifting from a 'just-in-time' approach to being 'just-in-case'.

We concluded that what is needed is a radical shift in the mindset of both public and Government. Preparedness and resilience in the face of major national crises must be normalised and seen as part of everyday life.

The Government should stop being squeamish about telling it straight to the public about the kind of threats we face. Evidence suggests that the public would reward honesty and openness with trust and reassurance, not fear and alarm.

This transformation to a state of realistic, informed readiness is not a short-term, one-off or tick-box project, but a long-term, continuous effort to ensure that every citizen understands their responsibility in helping to prevent emergencies and the role they should play should one occur. The same mindset applies whether the threat is war or a power cut, a cyber-attack or a pandemic, flood or a food shortage.

For all these reasons, our inquiry decided to focus on three objectives.

First, to update the context and governance of the UK's preparedness and resilience systems by raising the level of overall Government responsibility and accountability. Our recommendations include:

- the appointment of a Cabinet Minister solely responsible for resilience, supported by a Chief Resilience Officer at Permanent Secretary level;
- an annual statement on resilience to Parliament by the Prime Minister;
- the integration of local, voluntary, community and faith sectors, and the private sector, into the principal planning structure;
- a better command and control system to ensure the translation of top-level plans into co-ordinated, ground-level actions across the UK;
- regular publication of UK performance against the seven NATO civil preparedness baseline commitments, which the UK signed up to in 2016.

Secondly, to explain the interconnectedness of risks across different sectors and the systemic gaps which currently exist in critical strategic sectors. Our recommendations include:

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

- a statutory duty on private and public sector companies, organisations and services to conduct routine stress-testing exercises;
- the diversification of supply chains of critical strategic products including medicines, food and water, together with investment in rebuilding domestic manufacturing capacity in relevant sectors;
- examining the role and impact of cyber insurance, including its affordability for SMEs who are disproportionately damaged by cyber-attacks.

Thirdly, to understand the logistical and creative mechanics of building the 'whole-of-society' approach to resilience that is so often called for, including learning lessons from other countries with a significantly more advanced approach. Our recommendations include:

- statutory status and sustainable funding for Local Resilience Forums;
- education programmes to foster resilience skills, from primary school, through further and higher education, to adult and community learning;
- a national resilience course for senior leaders across society, modelled on Finland's national defence course;
- greater enrolment of civilian volunteers and reservists, including an expansion of the Armed Forces 'Gap Year' Foundation Scheme, to help generate a surge capacity from the population;
- databases and data sharing to ensure the inclusion of vulnerable individuals and groups in access to information and support in an emergency;
- withdrawal of the plan to switch off Digital Terrestrial Television, which would weaken universal access to communication in an emergency.

None of this will happen on its own. The Government, the Armed Forces and the emergency services cannot protect the entire population alone. Resilience must also be seen as an individual responsibility and a whole-of-society effort. Meeting the costs of effective preparedness is markedly cheaper than covering the costs of putting things right after a disaster. Recovery from cyber-attacks alone already costs us £14.7 billion a year.

Trust in central Government is at a low ebb. But the Government has already shown that it has the right ambition. What it needs now, before it's too late, is the leadership, the funding and the urgency to go with it.

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

Chapter 1: Introduction

1. *The Government must not treat emerging threats as distant or hypothetical problems. Doing so risks leaving the UK exposed as vulnerabilities develop. We recommend that where emerging risks or vulnerabilities are identified, the Government should act on them early by incorporating them into national risk assessments, preparedness plans and exercising, and by adapting capabilities as the threat develops.* (Paragraph 6)

2. Many of our witnesses called for a national conversation on resilience and preparedness; to engage the public and businesses and encourage people to take a more active role in preparing for emergencies. We therefore warmly welcome the Government's announcement of its three-year Be Ready campaign as an important step towards bringing people into that conversation and building a culture of preparedness across society. However, the take-up by the public and businesses will need to be assessed regularly, and the campaign must form part of a wider, long-term commitment to strengthening national resilience. The Government must provide sustained leadership and work closely with key stakeholders to ensure that public preparedness remains a national priority beyond the lifetime of the campaign. (Paragraph 22)

Chapter 2: Interconnected risks and threats

3. The absence of a clear, shared understanding of resilience risks undermining national preparedness, creating confusion about responsibilities and fragmenting efforts across Government, businesses and communities. Terms such as resilience and preparedness do not necessarily convey what is expected of individuals and households, highlighting the importance of clear, practical language in communicating how the public can prepare for emergencies. The Be Ready campaign is welcome in this regard. (Paragraph 33)

4. The UK's national resilience is seriously undermined by its limited domestic production and stockpiles of vital products, including food and medicines. This leaves the country dangerously exposed to disruption in global supply chains. We welcome the medical stockpiles maintained by DHSC and the contractual arrangements in place with suppliers and other partners, including the eight-week buffer stock requirement for secondary-care medicines. These arrangements provide important protection against disruption to medicines supply, although some stockpiles are maintained only for pandemic preparedness. (Paragraph 54)

5. *We welcome the establishment of the Supply Chain Centre. We recommend that the Government should set out its role, resourcing and how it will identify and address critical supply-chain dependencies, including how its effectiveness will be assessed.* (Paragraph 55)

6. *We recommend that the Government review whether existing stockpiles and supplier-held buffer arrangements provide sufficient coverage of medicines critical to national resilience, including during prolonged disruption. This review should clarify whether pandemic preparedness stockpiles can be deployed during other national emergencies, identify any gaps in coverage, and set out how these will be addressed. The Government should also invest in domestic production capacity for essential medicines and pharmaceutical ingredients, including 6-aminopenicillanic acid (6-APA), and work with the EU and other international partners to diversify and secure critical supply chains.* (Paragraph 56)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

7. *We recommend that the Government should set out how essential food and water supplies will be maintained during prolonged disruption. This should include strategic reserves for critical food and agricultural inputs, including fertilisers, stronger domestic production, and secure supply arrangements with the EU and other key partners. Water companies should also be required to demonstrate that they can maintain emergency supplies and distribution during prolonged outages.* (Paragraph 57)

8. The Government has begun to recognise the extent to which modern risks can interact, intensify one another and trigger consequences across multiple sectors. However, more must be done, and at greater pace, to ensure that this understanding is fully reflected in national preparedness arrangements. Too often planning and assurance remain organised in silos around individual risks, organisations and sectors rather than the continued operation of essential national functions. A failure originating in one system may therefore expose gaps in responsibility and preparedness across several others. (Paragraph 61)

9. *We recommend that the Government require the National Security Risk Assessment, National Risk Register, departmental preparedness plans and National Exercising Programme to assess and test scenarios involving interconnected risks and hybrid threats. These assessments and exercises should identify critical dependencies, responsible organisations, minimum levels of essential service, recovery priorities and unresolved capability gaps. The findings should be shared across the resilience system so that organisations can act on identified vulnerabilities, coordinate across sectors and address gaps before they are exposed in a crisis.* (Paragraph 62)

10. *We recommend that the Government report regularly to Parliament on the principal cross-sector vulnerabilities identified and the action being taken to address them.* (Paragraph 63)

11. We conclude that the existence of plans and frameworks is not, by itself, evidence of preparedness. They must not become compliance documents or "tick-box" exercises. The test is whether Government systems can operate effectively in practice on the ground, with clear responsibilities and arrangements that are understood, tested and capable of supporting timely and co-ordinated action. (Paragraph 66)

12. We welcome the Government's decision to establish expert panels to scrutinise preparedness for whole-system emergencies, but greater clarity is needed on their remit, operation and how their findings will inform cross-government preparedness and local operability. (Paragraph 67)

13. *We recommend that the Cabinet Office, within six months of publication of this report, establish a single national resilience strategy setting out clear working definitions of preparedness, resilience and national resilience, what is meant by a whole-of-society approach, and common outcomes, responsibilities and standards. Departmental, sectoral and local plans should be coordinated, consistent with the framework and regularly tested.* (Paragraph 68)

14. National resilience requires sustained, long-term investment in capabilities that are regularly tested, reviewed and improved. Investment in preparedness can be substantially less costly than responding to and recovering from a crisis. However, current funding and appraisal arrangements do not consistently recognise these potential savings or the long-term benefits of maintaining preparedness. (Paragraph 73)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

15. *We recommend that HM Treasury and the Cabinet Office should establish a multi-year funding and appraisal framework for national resilience. It should support the continuous maintenance, stress-testing, review and improvement of preparedness capabilities. Green Book guidance should require departments and public bodies to consider the cost of inaction, avoided future losses, cross-sector benefits and the long-term value of resilience measures when assessing investment proposals.* (Paragraph 74)

Chapter 3: Governance

16. The National Risk Register places too much emphasis on individual risks and not enough on their consequences, limiting its usefulness for understanding and preparing for interconnected disruption. (Paragraph 86)

17. Effective resilience depends on timely information sharing. Data sharing remains too fragmented and inconsistent for a complex and fast-moving risk environment, risking vulnerable individuals and groups being inadequately informed and supported during an emergency. (Paragraph 87)

18. *We recommend that the Government reflect the interdependent nature of many of the risks currently in the 2026 National Risk Register by consolidating these into a shorter list. It should give less emphasis in the National Risk Register to the causes of risks, and more to their consequences and how these can be mitigated.* (Paragraph 88)

19. *We recommend that the Government establish arrangements for sharing relevant and timely threat intelligence with designated, security-cleared personnel at critical national infrastructure operators. This should enable operators to better understand emerging threats, identify potential cascading impacts and take appropriate action to strengthen their resilience.* (Paragraph 89)

20. The Government has not translated its whole-of-society ambition into consistent operational practice. Local Resilience Forums, the private sector, voluntary and community organisations, and bodies in the devolved administrations are still not included in forward planning early or consistently enough. (Paragraph 103)

21. The Government seemed deficient in a clear command and control mechanism for translating top-down decision-making into lower-level delivery uniformly across the country. (Paragraph 104)

22. *We recommend that the Government strengthen command and control between national (gold command) and local (bronze command) resilience structures before, during and after national emergencies. Developing middle-level (silver command) management, of the kind that exists in Scotland, should aim to translate national plans into local action, co-ordinate resources and volunteers, and oversee preparedness and performance. The Government should establish regional co-ordination centres across the UK, using existing structures if possible.* (Paragraph 105)

23. We were not convinced that Government structures concerning resilience are adequate to achieve the co-ordination required. The Lead Government Department model provides accountability and expertise but does not adequately address cross-departmental risks and competing priorities. Current ministerial arrangements also lack the seniority and capacity needed to provide sustained leadership and drive improvements with sufficient urgency. (Paragraph 114)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

24. *We recommend that within six months of publication of this report, the Government should appoint a cabinet minister responsible solely for resilience, who should chair the National Security Council Sub-Committee on Resilience. The Minister should be assisted by a Chief Resilience Officer at Permanent Secretary level. It should also appoint an official as Head of Preparedness in every department to support the Permanent Secretary on preparedness and security and co-ordinate preparedness within the department.* (Paragraph 115)

25. *We recommend that the Prime Minister make an annual statement to Parliament on the state of the UK's preparedness, setting out progress made in strengthening national resilience and outlining the Government's priorities for the year ahead.* (Paragraph 116)

26. Artificial intelligence presents a further challenge to national resilience, amplifying existing threats and creating new vulnerabilities. Effective governance and regulation are essential to manage these risks and harness its potential benefits. (Paragraph 132)

27. The Government's legislative programme is not keeping pace with the resilience challenges identified by this inquiry. The Civil Contingencies Act 2004 provides a statutory framework, but Category 2 responders do not always engage as required. The Cyber Security and Resilience (Network and Information Systems) Bill would provide useful baseline requirements, but its scope is limited, while the Defence Readiness Bill has been delayed despite the importance of its subject matter. (Paragraph 133)

28. *We recommend that the Government remove the distinction under the Civil Contingencies Act 2004 between Category 1 and Category 2 responders, giving all of them the responsibilities of current Category 1 responders. It should change the wording that "encourages" engagement with wording that "requires" engagement with the Voluntary, Community and Faith Sector and the private sector.* (Paragraph 134)

29. *We recommend that the Government widen the scope of cyber security regulation beyond the provisions of the Cyber Security and Resilience (Network and Information Systems) Bill, ensuring that regulators have sufficient resources and capacity to enforce requirements effectively. It should also keep the regulatory framework under continuous review and update it regularly to reflect evolving cyber threats and technological developments.* (Paragraph 135)

30. *We recommend that the Government bring forward the Defence Readiness Bill as a matter of urgency to establish clear statutory responsibilities for national resilience across society. The Bill should place Local Resilience Forums on a statutory footing, with clear command and control status, provide for sustainable funding and strengthen accountability for preparedness at national and local levels.* (Paragraph 136)

31. The Government has not demonstrated that the UK currently meets its NATO civil preparedness commitments in practice. We received no clear evidence showing the extent to which the seven baseline requirements are met, how compliance is assessed, or how gaps are addressed. This lack of transparency prevents effective parliamentary scrutiny of the UK's preparedness against commitments it has undertaken. (Paragraph 143)

32. *We recommend that the Government publish UK performance against all seven NATO civil preparedness baselines and explain the improvements that will be made where requirements have not been met. It should monitor international frameworks*

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

on resilience, particularly EU legislation and directives, and apply these in the UK where relevant. (Paragraph 144)

Chapter 4: Activating the whole of society

33. The public, including young people, has demonstrated a strong willingness to contribute during national emergencies, but this has not yet been translated into consistent levels of preparedness. The evidence shows that resilience depends on turning willingness, plans and institutional responsibilities into coordinated capability across Government and wider society. This requires clear roles, practical skills and arrangements that work together in practice. (Paragraph 151)

34. Politicians and officials need to trust the public and take them into their confidence as much as security will allow, while offering them opportunities to play a fuller role as active citizens in response and recovery. The Government's Be Ready campaign marks a welcome step in this direction, but sustained, serious and measured communication from political leaders will be essential to building public confidence. (Paragraph 152)

35. While we welcome the action taken by the Government through its Be Ready campaign to improve public preparedness, we conclude that its other aims under Objective 2 of the 2025 Resilience Action Plan remain vague and fail to establish clear responsibilities for delivery. We are concerned that activity under the Plan is being treated as progress without evidence that the country is better prepared. (Paragraph 159)

36. The UK does not need to build its whole-of-society capability from scratch. Existing local authorities, community organisations, cultural institutions and voluntary groups already provide much of the infrastructure needed. The problem is that this capability is not yet consistently recognised or integrated into the national resilience system, nor is it supported by statutory arrangements or sustained funding. Civil society remains too often an emergency add-on, rather than a standing national capability. (Paragraph 160)

37. *We recommend that the Government should make local empowerment a central principle of its resilience approach. It should go beyond the Be Ready campaign and take active measures to support communities and businesses in their resilience preparations by enabling decisions to be taken at the lowest appropriate level within a clear national strategy and shared objectives.* (Paragraph 165)

38. *We recommend that the Government review whether existing Local Resilience Forums in England and Wales, Regional Resilience Partnerships in Scotland, and Emergency Preparedness Groups in Northern Ireland provide sufficient coverage to support whole-of-society resilience at community level. It should work with local authorities, involving community organisations, to ensure that the support needed for people who are vulnerable for a variety of reasons is available.* (Paragraph 166)

39. The private sector is not adequately integrated into national and local resilience planning. Businesses operate most of the infrastructure, logistics and supply chains on which the country depends, but their representation within resilience structures has been inconsistent or ignored. (Paragraph 178)

40. *We recommend that the Government establish a tiered framework for business resilience, proportionate to the criticality, size and risk profile of organisations. Tier 1 should be for businesses whose continued operation is essential to national resilience,*

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

which should be subject to statutory preparedness and continuity duties and regular stress tests. Tier 2 should be for organisations for whom statutory duties are not necessary, where the Government should use contractual arrangements to set and assure appropriate resilience requirements. Tier 3 should be for the wider business community, including SMEs, whose preparedness should be supported through voluntary, practical and sector-specific guidance, incentives such as tax reliefs and cheaper insurance for compliant businesses and opportunities to participate in resilience planning and exercising. The Government should clearly define which businesses fall within each tier and what is expected of them. (Paragraph 179)

41. *We recommend that the Government ensure that businesses of all sizes and public authorities recognise cyberattacks as a significant risk to their operations and take appropriate steps to strengthen their resilience. This should include promoting greater awareness of cyber risks and the role that insurance can play in mitigating their financial consequences, alongside practical measures to prevent, withstand and recover from attacks.* (Paragraph 180)

42. *We recommend that the Government ensure that Flood Re, a world first reinsurance scheme providing homeowners with affordable insurance, is extended beyond its planned end date of 2039. It should adapt public-private reinsurance models to provide more effective cover for risks that are difficult to insure, including large-scale cyber-attacks.* (Paragraph 181)

43. Education and training are fundamental to building a more resilient society, yet practical preparedness and resilience skills are not sufficiently embedded across the population. These capabilities should be developed throughout life rather than treated as specialist knowledge for resilience professionals. (Paragraph 191)

44. National resilience also increasingly depends on specialist technological capability. The UK's reliance on AI, cloud, cyber and other emerging technologies creates a need to build and retain domestic expertise while reducing critical dependencies on overseas providers. (Paragraph 192)

45. *We recommend that the Government develop a life-long national programme for resilience education and skills. This should embed practical preparedness, critical thinking and information literacy from an early age and reinforce these skills through further and higher education, workplaces and community learning. It should include the skills needed to identify and respond to misinformation and disinformation.* (Paragraph 193)

46. *We recommend that the Government expand the reach of the UK Resilience Academy beyond the public sector, with substantially greater participation from businesses and civil society. UKRA should establish a national resilience course for senior leaders, modelled on Finland's national defence courses, bringing together chief executives, directors, senior officials, parliamentarians, media professionals and leaders from civil society and faith organisations to build relationships and shared preparedness before crises occur.* (Paragraph 194)

47. *We recommend that the Government develop a programme to strengthen specialist skills in AI, cloud, cyber and other emerging technologies critical to national resilience. This should build and retain domestic technical capability, reduce critical dependencies on overseas providers and ensure that emerging technological risks are identified and addressed.* (Paragraph 195)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

48. *We recommend that the Government and the Armed Forces step up the plans to expand the Armed Forces 'Gap Year' Foundation Scheme with a vigorous public information campaign including targeting all those who are currently not in education, employment or training.* (Paragraph 196)

49. We welcome the increase in national exercising, including plans to test a wider range of threats and involve organisations across society. Exercises are most valuable when they expose weaknesses before a real emergency. We agree with the evidence that exercising should provide a safe environment in which organisations can "fail and learn". National exercises should therefore be sufficiently demanding to identify where plans, systems and cross-sector dependencies break down. (Paragraph 203)

50. It is not clear who is responsible for setting standards for resilience stress testing, assessing performance and ensuring that lessons identified through exercises are implemented. (Paragraph 204)

51. *We recommend that the Government apply the stress-testing approach used in the financial sector to national resilience. It should establish regular cross-sector stress tests for critical sectors, including food, energy and water, pharmaceuticals and other strategically important industries, involving central and local Government, the Armed Forces, Local Resilience Forums, the voluntary and community sector, and relevant businesses. It should also set out who will oversee this regime, including whether an existing regulator or a dedicated body should be responsible for setting standards, monitoring compliance and ensuring that lessons are acted upon.* (Paragraph 205)

52. Military reservists, veterans and other skilled volunteers could provide valuable additional capacity during national emergencies. However, we are concerned that the same individuals may be relied upon simultaneously by the Armed Forces, emergency services, healthcare and voluntary organisations. Without a clear understanding of these competing demands, resilience plans risk overstating the personnel available during a major or concurrent crisis. (Paragraph 214)

53. *We recommend that a national register of volunteers and civil reservists, focused on specialist skills and knowledge, should be developed and maintained. This should be developed through a national campaign and modelled on the NHS Volunteer Responders programme developed in COVID-19. The data exist but need to be reconfigured to identify existing volunteers, recruit new ones and ensure that they are given things to do in a crisis.* (Paragraph 215)

54. *We recommend that the Government explore the introduction of an entitlement to paid civic resilience leave, enabling employees to undertake approved training, exercising and emergency volunteering without loss of income. It should work with employers to establish proportionate arrangements and encourage wider participation across the workforce.* (Paragraph 216)

55. *We recommend that the Government require local authorities, working with Local Resilience Forums and voluntary and community organisations, to establish and maintain registers of local volunteers. These should identify relevant skills and capabilities and enable volunteers to be mobilised quickly and effectively during emergencies.* (Paragraph 217)

56. The move towards multi-year funding for Local Resilience Forums is welcome, but local resilience has too often depended on short-term and

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

fragmented funding. Effective local resilience depends on sustained and predictable investment that enables local structures to retain skilled staff, build enduring partnerships and develop capability. (Paragraph 221)

57. *We recommend that the Government set out a clear plan for how part of the 1.5% of GDP specified for 2035 will be spent on civil preparedness and resilience. It should break down planned spending and explain how resources will be allocated.* (Paragraph 222)

58. The Government is right to rebuild its home defence arrangements, but the relationship between civilian resilience and military defence remains underdeveloped. In a major conflict, civilian institutions are likely to have to support military operations while maintaining essential services, yet the responsibilities and arrangements involved are not sufficiently defined or tested. (Paragraph 227)

59. While the UK does not need to replicate other countries' total defence models, there is much to learn from their approaches to integrating civilian and military preparedness, particularly given the shared threats we face. (Paragraph 228)

60. *We recommend that the Government use the Home Defence Programme to define how civilian and military preparedness will work together in practice. It should clarify the roles of government, local responders, critical infrastructure operators and other civilian partners in supporting defence and test these arrangements through regular training and cross-government exercises.* (Paragraph 229)

Chapter 5: Communications and developing a culture of resilience

61. Despite recent promising developments contained within the Be Ready campaign, the Government has failed to communicate national risks openly and consistently enough. Reluctance to discuss serious threats leaves people less prepared, undermines public trust and creates opportunities for misinformation and disinformation to spread. Poorly judged or inconsistent communication also risks provoking public backlash on social media, particularly where trust in Government is already low. (Paragraph 245)

62. *We recommend that the Government adopt a more open approach to communicating national risks. It should provide regular, accessible and candid information about significant risks, their potential consequences and the actions being taken to mitigate them.* (Paragraph 246)

63. *We welcome the Prime Minister's announcement of the new National Centre for Information Defence. However, we recommend that the Government must clarify its remit, responsibilities and how it will operate in practice. The Centre should be operationally independent and take a proactive approach to identifying, attributing and countering hostile information activity, working closely with international partners.* (Paragraph 247)

64. *We recommend that the Government engage with a wide range of news outlets, including those which are not necessarily their natural partners, but which segments of the public trust, so key messages are heard by and reinforced to as many people as possible.* (Paragraph 248)

65. National resilience is heavily reliant on digital communication, but the supporting infrastructure remains vulnerable to power outages and/or damage to subsea cables. Existing mitigations are not yet sufficiently rigorous

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

or enduring to guarantee communications through prolonged disruption. Older technologies also remain important where digital communications fail, making the Government's dependence on digital systems without comprehensive back-up arrangements a significant resilience weakness. (Paragraph 258)

66. *We recommend that the Government develop, with the telecommunications and digital infrastructure sectors, a response plan in the event of widespread national power outages, subsea cable disruption, and any other means of interference, which sets out plans for the deployment of resilient back-up communications across different scenarios, and mandates regular testing of business continuity arrangements. The Government should also bring forward legislation to implement the proposals in its October 2026 White Paper on Critical Undersea Infrastructure Security and Resilience.* (Paragraph 259)

67. *We recommend that the Government should abandon its plan to switch off Digital Terrestrial Television, which risks weakening national resilience by reducing universal access to communication, as well as learn lessons from the switching off of the Public Switched Telephone Network on 31 January 2027.* (Paragraph 260)

68. A Government website is inadequate as the principal means of communicating resilience advice. Reliance on digital guidance risks excluding some groups, particularly during power or internet outages. The advice is also insufficient for prolonged or severe disruption. (Paragraph 275)

69. *We recommend that the Government should use its planned public preparedness campaigns, such as the Be Ready campaign, to make resilience and practical readiness a normal part of everyday life, strengthening civic responsibility and psychological preparedness, and encouraging individuals and households to take sustained action to prepare for emergencies.* (Paragraph 276)

70. *We recommend that the Government use its Be Ready campaign to deliver clear public preparedness communications, working through trusted local networks and tailoring messaging to different groups, including young people, vulnerable people, and those whose first language is not English or Welsh. The Government should ensure that there is a sustainable pipeline of qualified Public Service Interpreters and translators to support this.* (Paragraph 277)

71. *We recommend that the Government should distribute a booklet to every household, modelled on the Danish and Swedish equivalents, providing practical guidance on what to do during a crisis and the support people can expect from national and local Government and local community responders. This should be complemented by a multilingual public preparedness app, modelled on Finland's 112 Suomi app, enabling people to contact emergency services with their location transmitted automatically, receive official warnings targeted to their area, and access guidance on preparing for and responding to emergencies.* (Paragraph 278)

72. *We recommend that the Government require local resilience arrangements to identify, maintain and publicise accessible local stocks of food, water and other vital products for people who require these. The Government should also help local Government to establish a volunteer system to deliver essential supplies directly to those who are unable to obtain them themselves because of distance, illness, disability or other barriers.* (Paragraph 279)

73. Overall readiness remains inadequate and uneven across communities and sectors. There are examples of good practice, but too many businesses appear

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

insufficiently engaged with national resilience imperatives. Decisions made by the Government and business continue to give insufficient weight to long-term systemic risks in favour of short-term priorities and convenience. (Paragraph 287)

74. *We recommend that within six months of publication of this report, the Government should require each Local Resilience Forum to establish and maintain operational registers of suitable public and private buildings that can be used as shelters or community resilience hubs in the event of emergencies such as flooding or a prolonged power cut. These should record capacity, facilities, accessibility, and power arrangements, and identify local storage facilities holding critical food, water, medicines, and other vital products.* (Paragraph 288)

75. National resilience requires a fundamental shift in how the country understands and prepares for risk. Preparedness must become a national priority, embedded in the decisions and actions of Government, businesses, communities and individuals. The measure of success will not be the number of initiatives announced, but whether the UK is demonstrably better equipped to withstand disruption, protect its population and maintain the essential functions of society. (Paragraph 289)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Are we ready? Building a culture of resilience

CHAPTER 1: INTRODUCTION

1. The Government defines resilience as the ability to "anticipate, assess, prevent, mitigate, respond to, and recover from" natural hazards, deliberate attacks and other disruptive events or "threats to our way of life".[2] A recurring theme in the evidence was the need for preparedness to evolve as risks change and for plans and capabilities to be regularly reviewed, stress-tested and adapted. BT Group warned of a tendency "to prepare for the last resilience scenario, rather than taking a truly forward-looking approach".[3]

This inquiry

2. The House of Lords Select Committee on National Resilience was appointed on 27 January 2026 to consider national resilience, including the role of local resilience.

3. Our inquiry examined national resilience as a system. It did not seek to produce an exhaustive catalogue of every risk facing the UK or to assess the detailed operational plan for each one. Nor could we examine every infrastructure sector, public service or emergency capability in equal depth. Instead, we considered the common systemic weaknesses and capabilities which affect the country's ability to prepare for a wide range of emergencies.

4. Although we did not examine every individual risk in detail, this should not overlook the need to prepare for risks that are developing rapidly or difficult to predict. The Government's National Security Strategy identifies technological developments including artificial intelligence, engineering biology and quantum computing as sources of both opportunity and new vulnerability.[4] The Strategic Defence Review has also warned of new nuclear risks and rapid technological change affecting the nature of conflict.[5] The Overseas Territories must be fully integrated into national resilience planning, particularly given the risks they may pose in an unpredictable geopolitical environment.

5. Risks such as artificial intelligence and nuclear risks remain highly uncertain, but their potential consequences could be severe. In October 2026, the Director General of MI5, Sir Ken McCallum, warned that AI is already enhancing cyber threats and being exploited by terrorists to improve attack planning, with the potential to facilitate the development of biological weapons.[6] The possibility of nuclear escalation also remains among the most serious risks facing the UK.[7]

---

2 Cabinet Office, *UK Government Resilience Action Plan*, 8 July 2025, para 6
3 Written evidence from BT Group (NLR0141)
4 Cabinet Office, *National Security Strategy 2025: Security for the British People in a Dangerous World* , 24 June 2025
5 Ministry of Defence, *The Strategic Defence Review 2025: Making Britain Safer: secure at home, strong abroad*, 2 June 2025
6 MI5, MI5 Director General Delivers Annual Threat Update
7 Ministry of Defence, *The Strategic Defence Review 2025: Making Britain Safer: secure at home, strong abroad*, 2 June 2025

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

6. ***The Government must not treat emerging threats as distant or hypothetical problems. Doing so risks leaving the UK exposed as vulnerabilities develop. We recommend that where emerging risks or vulnerabilities are identified, the Government should act on them early by incorporating them into national risk assessments, preparedness plans and exercising, and by adapting capabilities as the threat develops.***

7. We launched our call for evidence on 9 March 2026. We sought evidence on:

- the risks and threats for which the UK should prepare;
- the interconnectedness of risks across sectors, countries and timeframes;
- the respective roles of central and local government, the private sector, civil society and the public;
- how risks should be communicated to businesses, communities and individuals;
- the preparedness of young people and vulnerable groups;
- barriers to long-term investment in resilience;
- the adequacy of the legislative and institutional arrangements governing resilience; and
- lessons which could be learned from other countries.

8. Significant aspects of emergency preparedness, response and recovery are devolved, while other responsibilities remain reserved to the UK Government. Risks and emergencies frequently cross these boundaries, requiring close co-operation between the UK Government and the devolved Governments of Scotland, Wales and Northern Ireland. The Government has established a Four Nation Ministerial Group to discuss and align resilience matters across the UK.[8] We received evidence from across the United Kingdom and have indicated where our recommendations relate specifically to the UK Government or require collaboration with the devolved Governments.

Other relevant work and inquiries

9. A substantial body of work on national risk and resilience preceded our inquiry. The most significant recent House of Lords report was *Preparing for Extreme Risks: Building a Resilient Society*, published by the Select Committee on Risk Assessment and Risk Planning in December 2021.[9]

10. The 2021 Committee concluded that the UK was insufficiently prepared for complex and unfamiliar risks, particularly where failures could cascade across interconnected systems. It criticised opaque risk policymaking and excessive secrecy and found that the Government had not yet achieved a whole-of-society approach to resilience.[10]

11. It recommended more open risk communication, stronger engagement with local and non-government actors, more regular testing of plans, and a more

8 Written evidence from Cabinet Office (NLR0126); Scottish Government (NLR0169)
9 Select Committee on Risk Assessment and Risk Planning, *Preparing for Extreme Risks: Building a Resilient Society* (Report of Session 2021–22, HL Paper 110)
10 *Ibid.*

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

dynamic approach to risk assessment. It also proposed an independent Office for Preparedness and Resilience, led by a Government Chief Risk Officer, to assess capability, set standards and scrutinise preparedness.[11]

12. The Government published its response in March 2022. It accepted or agreed in principle with a number of the Committee's recommendations and referred to work already under way to improve risk assessment, public communication and the involvement of organisations outside government. It did not accept the recommendation to establish an independent Office for Preparedness and Resilience.[12]

13. Our inquiry built on the 2021 report rather than repeating it. We did not conduct another detailed examination of the methodology used to calculate the likelihood and impact of individual risks. Nor did we reconsider each of the 2021 Committee's recommendations separately. Instead, we examined whether the changes made since that report had produced a clearer and more inclusive system of national preparedness.

14. The UK COVID-19 Inquiry has undertaken a detailed investigation of pandemic preparedness. Its Module 1 report, published in July 2024, examined the UK's central structures and procedures for preparing for and responding to a pandemic.[13] Our report does not reproduce that examination or seek to reassess the Government's pandemic plans. We considered the pandemic principally for the wider lessons it provides about national readiness, central and local co-ordination, public communication, volunteering and the consequences of failing to maintain sufficient capability before a crisis.

Government activity

15. Since the 2021 report, the Government has introduced a number of changes. In December 2022, it published the UK Government Resilience Framework, setting out how it intended to strengthen the structures and capabilities supporting national resilience. The Framework was based on three principles: developing a shared understanding of risk; placing greater emphasis on prevention and preparation; and treating resilience as a whole-of-society endeavour.[14]

16. In July 2025, the Government replaced the Framework with a Resilience Action Plan. The Action Plan set three objectives for the present Parliament: continuous assessment of the UK's resilience; enabling whole-of-society resilience; and strengthening the resilience system. It included commitments relating to risk assessment, national exercises, local resilience, Critical National Infrastructure, public preparedness and the involvement of businesses and voluntary organisations.[15]

17. In the same year, the Cabinet Office also combined the Resilience Directorate and COBR Unit into a single COBR Directorate, bringing together longer-

11 *Ibid.*
12 Cabinet Office, *Government response to Preparing for Extreme Risks: Building a Resilient Society*, 17 March 2022
13 UK COVID-19 Inquiry, *Module 1 Report: The resilience and preparedness of the United Kingdom*, 18 July 2024
14 Cabinet Office, *The UK Government Resilience Framework*, 19 December 2022
15 Cabinet Office, *UK Government Resilience Action Plan*, 8 July 2025

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

term resilience and crisis response.[16] Other developments included the establishment of the National Situation Centre, the Emergency Alerts service, the UK Resilience Academy, and reforms intended to strengthen Local Resilience Forums.[17] In January 2026, emergency alerts were issued to approximately 500,000 people across Cornwall and the Isles of Scilly during severe storms.[18] In August 2026, the system was used on a much larger scale, with an alert sent across England and Wales warning of a serious national wildfire risk.[19]

18. During our inquiry, the Government published its first implementation report on the Action Plan. This described progress against its commitments and reiterated the Government's intention to adopt an all-hazards and whole-of-society approach. It also acknowledged that the risk landscape continued to change and that preparedness depended on the continuing identification and assessment of emerging and longer-term risks.[20]

19. However, the continued introduction of new strategies, structures and commitments does not remove the need for scrutiny of their practical impact on the ground. Our inquiry examined how far these changes had altered preparedness in practice; whether responsibilities were understood outside the Cabinet Office; whether national plans were connected to local and sectoral arrangements; and whether the Government had established the leadership, resources and accountability needed to sustain its ambitions. The evidence we received exposed substantial weaknesses in the current resilience landscape, but also broad agreement on what needs to change.

20. Since the Committee agreed its report, the Government has published a public campaign called "Be Ready" which provides advice for how the public can prepare for everyday emergencies. The campaign replaces the previous Prepare website. The Government said that this campaign marks the first phase of a gradual roll out of its three-year campaign - part of a national conversation - designed to increase household resilience across the country. The advice will outline steps that households and individuals can take, including gradually stockpiling enough bottled water and food to last for three days and, for vulnerable people, signing up for support from energy suppliers, network operators, and water companies.[21]

21. The Government accepts "much of the advice has not changed and remains evergreen for households to follow."[22] It does not detail what discrete advice it has for communities and businesses but does say "More than five hundred organisations across the UK, from charities to businesses, have already signed-up to share messaging and campaign assets within their networks and communities."[23]

22. **Many of our witnesses called for a national conversation on resilience and preparedness; to engage the public and businesses and encourage**

16 Cabinet Office, *The UK Government Resilience Action Plan: 2026 Implementation Report*, 14 July 2026
17 Written evidence from the Cabinet Office (NLR0126)
18 Cabinet Office, *The UK Government Resilience Action Plan: 2026 Implementation Report*, 14 July 2026
19 The Guardian, *Emergency alert warning of wildfire risk sent to phones in England and Wales*, 14 August 2026
20 Cabinet Office, *The UK Government Resilience Action Plan: 2026 Implementation Report*, 14 July 2026
21 HM Government, *Be Ready*
22 Cabinet Office, *Households encouraged to take small, simple steps to stay prepared in an emergency*, 22 October 2026
23 *Ibid.*

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

people to take a more active role in preparing for emergencies. We therefore warmly welcome the Government's announcement of its three-year Be Ready campaign as an important step towards bringing people into that conversation and building a culture of preparedness across society. However, the take-up by the public and businesses will need to be assessed regularly, and the campaign must form part of a wider, long-term commitment to strengthening national resilience. The Government must provide sustained leadership and work closely with key stakeholders to ensure that public preparedness remains a national priority beyond the lifetime of the campaign.

Evidence and engagement

23. We received 169 written submissions. These came from government departments and public bodies; the devolved Governments and local authorities; emergency services and Local Resilience Forums; Critical National Infrastructure operators; businesses and professional bodies; voluntary, community and faith organisations; academics; charities; schools and youth organisations; and individual members of the public.

24. We heard oral evidence in 21 public panels. Witnesses included Ministers and officials from the Cabinet Office and other Government departments; former Ministers and senior officials; representatives of local Government, the emergency services and the Armed Forces; cyber-security and communications experts; infrastructure operators; businesses; voluntary organisations; academics; journalists; and the ambassadors of Denmark, Finland, Norway and Sweden.

25. The Government's national surveys of public attitudes towards risk, resilience and preparedness have so far focused on adults aged 18 and over. We considered that younger people also have an important stake in the country's resilience and therefore sought evidence reflecting their perspectives. On 4 June 2026, we held a private roundtable with students from universities across the United Kingdom. The discussion covered young people's understanding of national risks, the information and training available to them, trust in institutions, volunteering and the contribution that schools, universities and employers could make to preparedness. We also asked Pupils 2 Parliament to gather the views of pupils aged 11 to 17 from two state secondary schools, providing a further perspective on young people's understanding of national risks and their preparedness for emergencies.

26. We are grateful to everyone who gave evidence or otherwise assisted the inquiry. We are also grateful to our specialist adviser, Robert Hall, for his advice and support throughout our work, and to Lord Harris of Haringey, Chair of the National Preparedness Commission, for his valuable contribution and longstanding expertise in the field of national resilience. The full lists of written and oral evidence and of the Committee's engagement activities are set out in the appendices to this report.

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

CHAPTER 2: INTERCONNECTED RISKS AND THREATS

27. Is the UK prepared for a major, cross-sector crisis, or does resilience remain stronger on paper than in practice? This chapter considers whether the UK's current approach is sufficiently practical and sustained to meet an increasingly complex and interconnected risk landscape.

Defining resilience and responsibility

What is resilience?

28. For the purposes of this report, we use the Government's definition of resilience, set out in Chapter 1. We use preparedness to mean the plans, resources, capabilities, training and relationships put in place before an emergency. National resilience refers to the collective ability of Government, public services, infrastructure operators, businesses, voluntary organisations, communities and individuals to anticipate and reduce risks, withstand disruption, maintain essential functions, respond effectively, recover and adapt.

29. The Government takes an "all hazards" approach to resilience. Its evidence said that the resilience system includes risk assessment and prevention; the resilience of public services, essential services and Critical National Infrastructure; local resilience and community cohesion; skills, training and education; legislation, regulation and standards; public engagement; and specific capabilities or countermeasures for particular hazards.[24]

30. Witnesses told us that there was no agreed definition of resilience.[25] Rick Cudworth, Executive Director of Resilience First, told us that the language of resilience remained too reactive, focused on "writing plans, training and exercising, response, recovery". He argued that resilience should instead be understood through organisations' ability to "anticipate", "absorb" and "adapt".[26]

What does a whole-of-society approach mean?

31. The Centre for Whole of Society Resilience, a transdisciplinary network of academics, practitioners, business leaders and consultants working to advance research-informed resilience policy and practice, told us that in order to develop whole-of-society preparedness and resilience a shared vision "must be co-owned across central government, devolved administrations, local government, public services, business and civil society, because delivery depends on action and capability across the whole system."[27]

32. Norwegian Ambassador HE Tore Hattrem told us that "we do not separate private industry, civil society, independent institutions and defence because we realise that, in the challenges that will confront us in the future, everybody must play their role."[28]

---

24 Written evidence from Cabinet Office (NLR0126)
25 Q 11 (Helena Coe); written evidence from Anna Goodden, Dr James Porter and Dr Francesca Vantaggiato (NLR0062); Prof Stergios-Aristoteles Mitoulis, Prof Sotirios Argyroudis and Dr Nadiia Kopiika (NLR0063) and Grand Challenge AI (NLR0105)
26 Q 11 (Rick Cudworth)
27 Written evidence from the Centre for Whole of Society Resilience (NLR0119)
28 Q 18 (Tore Hattrem)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

33. **The absence of a clear, shared understanding of resilience risks undermining national preparedness, creating confusion about responsibilities and fragmenting efforts across Government, businesses and communities. Terms such as resilience and preparedness do not necessarily convey what is expected of individuals and households, highlighting the importance of clear, practical language in communicating how the public can prepare for emergencies. The Be Ready campaign is welcome in this regard.**

The changing risk landscape

34. Dame Angela Eagle MP told us that the UK was "pivoting into a different era" and moving from the post-Cold War peace dividend into "a much more hybrid hostile situation".[29] She attributed this change to "the increase in technological ability, the hybrid war that is going on at the moment, the cyberattacks and the attempts at foreign national interference".[30]

Chronic risks and acute risks

35. The Government's National Risk Register, 2025 states that "Chronic risks are distinct from acute risks in that they pose continuous challenges that erode our economy, community, way of life, and/or national security. Generally, but not always, these manifest over a longer timeframe."[31] It explains that acute risks "are risks that may require an emergency response from government, such as wildfires or biological attacks."[32]

36. The NAO highlighted the interaction between acute and chronic risks. Sian Jones warned that the £49 billion backlog in public property maintenance could become "an almost existential risk" due to a lack of sustained investment.[33]

Hostile and sub-threshold state activity

37. The Government's 2025 National Security Strategy warned of increasing hostile activity from states including Russia and Iran.[34] We are witnessing an escalating campaign of systematic hostility, coercion and destabilisation that goes well beyond conventional hybrid threats and attacks, while remaining below the threshold of open armed conflict.[35]

38. Lieutenant General Sir Charles Collins, Deputy Chief of the Defence Staff, told us that the UK's traditional approach of defending itself at a distance "no longer fully applies because long-range systems, hybrid warfare et cetera mean that we are in danger at home".[36] He stressed that national resilience required a "cross-Whitehall effort" in which "the military lever is only one part".[37]

39. This vulnerability at home also extends to missile threats. Lt-Gen Collins said that: "Ballistic missile protection is another area where we are reliant

29 Q 181 (Angela Eagle MP)
30 *Ibid.*
31 HM Government, *National Risk Register—2025 edition*, 16 January 2025
32 *Ibid.*
33 Q 2 (Sian Jones)
34 Cabinet Office, *National Security Strategy 2025: Security for the British People in a Dangerous World* (June 2025, CP 1338)
35 House of Commons Defence Committee, *Defence in the Grey Zone* (Session 2024–25, HC 405)
36 Q 78 (Charles Collins)
37 *Ibid.*

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

on NATO at the moment as we build our integrated air missile defence system, as promised in the SDR."[38] NATO's ballistic missile defence system combines NATO command-and-control arrangements with capabilities provided by individual Allies, including the United States. Lt-Gen Collins referred to planned investment and to the need to exercise the system with other Government departments and NATO allies.[39]

40. Finland's Ambassador, HE Teemu Turunen, described "constant hybrid-type activities" affecting Finland and its Nordic neighbours.[40] He said that Finland had consequently strengthened co-operation between the "border guard, police, military and civilian intelligence", and stressed that threats to critical infrastructure must include consideration of "undersea infrastructure and the shadow fleet".[41]

41. Cyber threats pose a growing risk to national resilience, with more than 90,000 attempted cyberattacks on the UK's defence systems in a single year.[42] Michael Brunton-Spall, Deputy Director of Cyber Services in the Government Cyber Unit, warned that the Government and wider public sector faced "critically high cyber and digital resilience risks", reflecting an "escalating threat environment" and "extremely low levels of resilience".[43] He highlighted the potential consequences for essential public services, warning that ransomware attacks on local authorities could "incapacitate social care systems", preventing front-line workers from accessing information needed to protect vulnerable people.[44]

International instability and supply-chain exposure

42. International instability can create or intensify domestic risks. The British Chambers of Commerce warned that conflict in the Middle East had disrupted shipping routes and increased energy prices, with prolonged conflict risking shortages of fuels and commodities and higher inflation.[45]

43. Bittium, a Finnish defence technology company, told us that global supply chains for semiconductors, advanced components, and secure communications technologies were exposed to "geopolitical shocks, export restrictions, and logistical constraints", and warned that disruption affecting one region or supplier could have disproportionate effects across several sectors.[46] The Met Office warned that, where several countries were repairing or replacing critical infrastructure simultaneously, the UK could face "extended lead times for essential components", particularly where it lacked the domestic capability to manufacture them.[47]

44. Sustain, an alliance of around 100 organisations working to improve the UK's food and farming system, told us that "the UK imports significant quantities of food, energy, and fertiliser from countries and regions that are increasingly politically unstable".[48] It said that recent international

38 *Ibid.*
39 *Ibid.*
40 Q 27 (Teemu Turunen)
41 *Ibid.*
42 Ministry of Defence, *The Defence Investment Plan*, 30 June 2026
43 Q 54 (Michael Brunton-Spall)
44 *Ibid.*
45 Written evidence from the British Chambers of Commerce (NLR0140)
46 Written evidence from Bittium (NLR0116)
47 Written evidence from the Met Office (NLR0120)
48 Written evidence from Sustain (NLR0152)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

conflicts had translated directly into higher food prices for UK households.[49] Professor Tim Lang, Professor Emeritus of Food Policy at the University of London, also said that the food system was heavily dependent on oil, gas and artificial fertilisers, and warned that concentrated supply chains could produce significant knock-on effects when disrupted.[50]

45. Witnesses raised concerns about the limited storage built into the food supply system. Baroness Batters, former President of the National Farmers' Union, warned that sudden changes in consumer behaviour could rapidly create shortages, as demonstrated during COVID-19.[51] Professor Lang wrote that "the UK has next to no national, regional or local systems of food storage".[52] He argued that asking households to store only a few days of food and water was "not dealing with the strategic risks to our food system".[53]

46. Evidence highlighted the need to identify and protect essential supplies and capabilities. ADS Group Ltd called for clearer stockholding requirements, including which goods should be held, where and in what quantities,[54] while the Society of Chemical Industry emphasised the importance of identifying industrial capabilities essential to national resilience that had been lost or were at risk.[55] Finland provides a more systematic model. Its National Emergency Supply Agency brings Government and businesses together in sector-specific preparedness groups, including one focused on grocery supply and distribution. These networks allow businesses and authorities to identify vulnerabilities, share information on emerging risks and maintain a common picture of security of supply (see Appendix 7).

47. Significant vulnerabilities also remain across medical device and pharmaceutical supply chains. Dr Peter Gogalniceanu, Director of Health Policy at Guy's Hospital, told us that surgical specialties had become dependent on equipment and consumables supplied from overseas. He warned that disruption to supplies of items such as robotic equipment, scissors and staplers could prevent commonly performed operations.[56] Mark Samuels, Chief Executive of Medicines UK, similarly warned of substantial overseas dependence in pharmaceutical supply chains and said that the UK was "in effect, entirely reliant on overseas antibiotics".[57]

48. We heard that greater domestic manufacturing could strengthen resilience but would not remove the UK's dependence on international supply chains. Mark Samuels told us: "It is always wise to manufacture domestically if you can. We will never manufacture everything here, so that means international relations are very important."[58]

49. NHS Supply Chain told us that it had identified around 350 frequently used products where there were risks to supply resilience. For these products, it

---

49 *Ibid.*
50 Q 116 (Prof Tim Lang)
51 Q 116 (Baroness Batters DL)
52 Written evidence from Prof Tim Lang and Antony So (NLR0145)
53 Q 118 (Prof Tim Lang)
54 Written evidence from ADS Group Ltd (NLR0040)
55 Written evidence from the Society of Chemical Industry (NLR0148)
56 Q 148 (Dr Peter Gogalniceanu)
57 Q 149 (Mark Samuels)
58 Q 171 (Mark Samuels)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

had increased stock levels to provide "six to eight weeks of stock in the UK available to distribute at any one time".[59]

50. The UK's approach to strategic medicines stockholding has changed considerably over time. The Essential Medicines Buffer Stock, established in 2009 to maintain an eight-week buffer of essential medicines, formally ended in 2019/20, with a small number of products retained until March 2022 as part of the COVID-19 Supportive Medicines stockpile.[60] The additional six-week stocks built ahead of the UK's departure from the EU are also no longer maintained.[61]

51. Some stockholding requirements remain in place. Since 2022, suppliers on NHS England's medicines procurement and supply chain (MPSC) frameworks have been required to hold an eight-week buffer of secondary-care medicines. Not all secondary-care medicines are covered by these frameworks, and the Government has acknowledged that compliance is not yet universal.[62] DHSC also maintains separate pandemic preparedness stockpiles, including antibiotics, antivirals, vaccines and other clinical supplies.[63]

52. We heard about international approaches to strengthening supply-chain resilience. Professor Lang described a Swiss model in which firms maintain strategic reserves with Government support.[64] The Critical Supply Group said that South Korea mandates "entities supplying critical sectors to increase stockpiling".[65] Sandoz said that: "Germany has taken the clearest steps to integrate value-based procurement into antibiotics purchasing" by reserving some contracts for products using ingredients sourced within the EU.[66] The NAO's September 2026 report on food supply-chain resilience found that Defra had not done enough to prepare for catastrophic disruption and recommended assessing whether approaches used in other countries could be applied in the UK.[67]

59 Q 173 (Andrew New)
60 Written evidence from Sandoz (NLR0125); HC Written Answer, 108288, Session 2022–23
61 Public Services Committee, *Medicines Security—a National Priority* (4th Report, Session 2024–26, HL Paper 252)
62 Written evidence from the Department of Health and Social Care and NHS (MED0043)
63 Department of Health and Social Care, *Stockpiles of medical products held by the Department of Health and Social Care*, 13 August 2026
64 Q 117 (Prof Tim Lang)
65 Written evidence from the Critical Supply Group (NLR0106)
66 Written evidence from Sandoz (NLR0125)
67 National Audit Office, *Resilience of the food supply chain to disruptions*, 4 September 2026

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Box 1: Supply chain vulnerabilities

The UK manufactures almost one quarter of its medicines, while approximately one third come from India and one third from the European Union; around half of active pharmaceutical ingredients come from China and half from India.[68] Two thirds of NHS generic medicines cost less than half the price of a first-class stamp for a month's supply, forcing manufacturers to seek the cheapest ingredients globally and making the system vulnerable to minor disruptions.[69]

Around 90% of global 6-APA, the critical precursor for penicillin-class antibiotics, is produced in China, while nearly 70% of antibiotic active pharmaceutical ingredient sites are located in China and India. Sustained price pressure and price-only procurement have driven most European producers from the market, leaving only one major fully integrated penicillin manufacturing network in Europe and no UK fallback following the closure of the last domestic plant in 2025.[70]

94.5% of British retail food is supplied by nine companies using 131 distribution hubs, meaning that disruption to a small number of dominant companies could produce substantial knock-on effects.[71] The food system operates on a just-in-time basis, with only two or three days of stock being held for some commodities.[72]

Carbon dioxide is a cross-cutting dependency across food manufacturing, retail and fertiliser production. Since it is used throughout the system, a break in supply could affect several sectors at once and transmit rapidly through the wider food chain.[73]

Food production is dependent on artificial nitrogen, phosphate and potash fertilisers. In the short term, the UK cannot readily replace these inputs and remains tied to imported supplies. Alternative approaches, such as organic production, biological nutrient cycles and recovering phosphates from waste, could reduce dependence but would require substantial infrastructure and time.[74]

Blood and blood products, including platelets and plasma, are critical during conflict or mass-casualty events. Resilience depends not only on collecting sufficient blood but also on preserving and transporting it around the country and manufacturing blood products. Disruption to logistics could restrict the blood types and blood products available where they are needed.[75]

Recent water outages in west Kent exposed weaknesses in the contingency supply chain. Bottled water had to be transported from distant locations, water companies lacked sufficient staff to operate distribution stations, and residents travelled long distances to find stocks exhausted within hours.[76]

53. The Government acknowledged the need to identify and manage critical supply-chain dependencies. The Security Minister at the time said: "We cannot produce absolutely everything on our own land … We have to make

68 Q 170 (Mark Samuels)
69 *Ibid.*
70 Written evidence from Sandoz (NLR0125)
71 Q 116 (Prof Tim Lang)
72 Q 118 (Prof Tim Lang)
73 Q 116 (Prof Tim Lang)
74 Q 117 (Prof Tim Lang)
75 Q 152 (Dr Peter Gogalniceanu)
76 Q 1 (Matt Boughton)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

strategic decisions".[77] She added that the Government had been identifying "critical bottlenecks and weak points" and had established a Supply Chain Centre in the Department for Business and Trade (DBT).[78]

54. **The UK's national resilience is seriously undermined by its limited domestic production and stockpiles of vital products, including food and medicines. This leaves the country dangerously exposed to disruption in global supply chains. We welcome the medical stockpiles maintained by DHSC and the contractual arrangements in place with suppliers and other partners, including the eight-week buffer stock requirement for secondary-care medicines. These arrangements provide important protection against disruption to medicines supply, although some stockpiles are maintained only for pandemic preparedness.**

55. ***We welcome the establishment of the Supply Chain Centre. We recommend that the Government should set out its role, resourcing and how it will identify and address critical supply-chain dependencies, including how its effectiveness will be assessed.***

56. ***We recommend that the Government review whether existing stockpiles and supplier-held buffer arrangements provide sufficient coverage of medicines critical to national resilience, including during prolonged disruption. This review should clarify whether pandemic preparedness stockpiles can be deployed during other national emergencies, identify any gaps in coverage, and set out how these will be addressed. The Government should also invest in domestic production capacity for essential medicines and pharmaceutical ingredients, including 6-aminopenicillanic acid (6-APA), and work with the EU and other international partners to diversify and secure critical supply chains.***

57. ***We recommend that the Government should set out how essential food and water supplies will be maintained during prolonged disruption. This should include strategic reserves for critical food and agricultural inputs, including fertilisers, stronger domestic production, and secure supply arrangements with the EU and other key partners. Water companies should also be required to demonstrate that they can maintain emergency supplies and distribution during prolonged outages.***

Cross-sector dependencies

58. The Alan Turing Institute told us that the energy, transport, communications and finance sectors were "tightly coupled" and that disruption in one "frequently spreads rapidly to others".[79] It cited the 2024 CrowdStrike outage as an example of a single software failure affecting aviation, healthcare, banking and emergency services.[80] Sophie Greaves, Associate Director for Digital Infrastructure at techUK, highlighted the mutual dependence between electricity and communications, telling us that "if there is no electricity, there is no network".[81]

77 Q 188 (Angela Eagle MP)
78 *Ibid.*
79 Written evidence from the Alan Turing Institute (NLR0091)
80 *Ibid.*
81 Q 116 (Sophie Greaves)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

59. Cyber incidents illustrated the risks arising from shared dependencies particularly clearly. Oliver Neuberger, Managing Director of Accenture, warned that a single cyber incident could affect "thousands of people and suppliers" because of shared technologies, legacy systems and reliance on third-party services. He identified cloud technology as a common dependency across organisations, increasing the potential for disruption to spread.[82]

60. PwC UK identified a significant information imbalance between Government and infrastructure operators. It said that operators held "detailed real-time insight into system performance, supply chain fragility and operational dependencies", while parts of Government had visibility of "cross-sector risks, geopolitical/economic pressures, and national security intelligence" that operators could not access.[83] Consequently, "neither side has a complete picture of the systemic vulnerability", making it difficult to assess cascading effects, resolve trade-offs or prioritise recovery.[84]

61. **The Government has begun to recognise the extent to which modern risks can interact, intensify one another and trigger consequences across multiple sectors. However, more must be done, and at greater pace, to ensure that this understanding is fully reflected in national preparedness arrangements. Too often planning and assurance remain organised in silos around individual risks, organisations and sectors rather than the continued operation of essential national functions. A failure originating in one system may therefore expose gaps in responsibility and preparedness across several others.**

62. ***We recommend that the Government require the National Security Risk Assessment, National Risk Register, departmental preparedness plans and National Exercising Programme to assess and test scenarios involving interconnected risks and hybrid threats. These assessments and exercises should identify critical dependencies, responsible organisations, minimum levels of essential service, recovery priorities and unresolved capability gaps. The findings should be shared across the resilience system so that organisations can act on identified vulnerabilities, coordinate across sectors and address gaps before they are exposed in a crisis.***

63. ***We recommend that the Government report regularly to Parliament on the principal cross-sector vulnerabilities identified and the action being taken to address them.***

Plans, strategies and frameworks

64. Throughout our inquiry, the Government and other witnesses described numerous plans, strategies, assessment processes and operational frameworks relevant to preparedness and resilience. Evidence from the Cabinet Office referred, among other arrangements, to the Resilience Action Plan, National Security Risk Assessment, National Risk Register, National Capabilities Assessment, Amber Book, Biological Security Strategy, Home Defence Programme and National Exercising Programme.[85] Witnesses understandably questioned whether the Government's arrangements were coherent. The

82 Q 54 (Oliver Neuberger)
83 Written evidence from PwC UK (NLR0094)
84 *Ibid.*
85 Written evidence from Cabinet Office (NLR0126)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Red Thread Collective described "a proliferation of frameworks" covering overlapping territory, with inconsistent concepts and non-interoperable assessment methods, which it said prevented a clear national picture of resilience capability and gaps.[86] The Security Institute similarly concluded that the UK "does not lack capability—it lacks coherence".[87]

65. The Government told us that this system was complex but comprehensive. It said that the Cabinet Office led on cross-cutting and catastrophic risks, while departments retained responsibility for risks within their areas of expertise. It also said that the Cabinet Office had strengthened its leadership role for crises with major cross-sector effects and was establishing expert panels to scrutinise preparedness for whole-system emergencies.[88]

66. **We conclude that the existence of plans and frameworks is not, by itself, evidence of preparedness. They must not become compliance documents or "tick-box" exercises. The test is whether Government systems can operate effectively in practice on the ground, with clear responsibilities and arrangements that are understood, tested and capable of supporting timely and co-ordinated action.**

67. **We welcome the Government's decision to establish expert panels to scrutinise preparedness for whole-system emergencies, but greater clarity is needed on their remit, operation and how their findings will inform cross-government preparedness and local operability.**

68. ***We recommend that the Cabinet Office, within six months of publication of this report, establish a single national resilience strategy setting out clear working definitions of preparedness, resilience and national resilience, what is meant by a whole-of-society approach, and common outcomes, responsibilities and standards. Departmental, sectoral and local plans should be coordinated, consistent with the framework and regularly tested.***

Long-term preparedness

69. A recurring theme in the evidence was that resilience requires sustained commitment and continuous adaptation, rather than one-off planning. The Continuity Forum called for "a culture of continuous preparedness"[89] and warned that point-in-time assessments could mask "persistent fragility" where organisations prepared for audits rather than maintaining capability continuously.[90] Ambassador Turunen told us that preparedness was "not a sprint, but a marathon" and was "more of a mindset than a short period of preparedness".[91] Emerging Risks Global said that preparedness arrangements should be "regularly reviewed" and "adapted to emerging threats".[92]

70. The case for investing before a crisis occurs was made repeatedly in evidence and has also been recognised by the Government. The UK Government Resilience Framework acknowledged that the majority of Government expenditure on emergencies was directed towards response and recovery

86 Written evidence from Red Thread Collective (NLR0110)
87 Written evidence from the Security Institute (NLR0071)
88 Written evidence from Cabinet Office (NLR0126)
89 Written evidence from the Continuity Forum (NLR0049)
90 *Ibid.*
91 Q 18 (Teemu Turunen)
92 Written evidence from Emerging Risks Global (NLR0002)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

rather than longer-term prevention and preparation, despite the cost of responding to and recovering from emergencies often outweighing the cost of preparing for or preventing them.[93] It cited Environment Agency analysis showing that every £1 spent advising on flood risk in planning applications had saved £12 in future flood damages.[94] The costs of failing to prepare are also already substantial. Ed de Minckwitz cited KPMG analysis estimating that cyberattacks cost the UK economy £14.7 billion a year.

71. The Treasury's Green Book was revised in February 2026 and now explicitly requires appraisal to consider the costs of preventing or mitigating risks alongside the impact and corrective costs that such investment could avoid.[95]

72. Witnesses also proposed ways to address short-termism in preparedness. The Emergency Planning Society said that "small, short-term grants" were administratively burdensome and "unlikely to create durable capability"; funding should instead be "proportionate, multi-year and linked to outcomes", including training, exercising and mutual-aid arrangements.[96]

73. **National resilience requires sustained, long-term investment in capabilities that are regularly tested, reviewed and improved. Investment in preparedness can be substantially less costly than responding to and recovering from a crisis. However, current funding and appraisal arrangements do not consistently recognise these potential savings or the long-term benefits of maintaining preparedness.**

74. ***We recommend that HM Treasury and the Cabinet Office should establish a multi-year funding and appraisal framework for national resilience. It should support the continuous maintenance, stress-testing, review and improvement of preparedness capabilities. Green Book guidance should require departments and public bodies to consider the cost of inaction, avoided future losses, cross-sector benefits and the long-term value of resilience measures when assessing investment proposals.***

93 Cabinet Office, *The UK Government Resilience Framework*, 19 December 2022
94 *Ibid.*
95 HM Treasury, *The Green Book 2026*, 5 February 2026
96 Written evidence from the Emergency Planning Society (NLR0118)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

CHAPTER 3: GOVERNANCE

75. Who is ultimately responsible for national resilience and who do we hold to account? This chapter considers whether current arrangements provide the leadership, accountability and co-ordination needed to turn resilience policy into action.

76. A fundamental responsibility of Government is to provide effective national command and control, ensuring clear direction and co-ordinated action across the resilience system. Yet the evidence we received revealed significant weaknesses in the Government's ability to fulfil this responsibility.

Risk assessment

77. The Government maintains a National Risk Register (NRR) to assess significant risks to the UK. The 2026 version identifies 95 "acute" risks, comprising 87 standalone risks and eight linked scenarios, which could require an emergency response. It assesses the likelihood and impact for each risk and sets out a "reasonable worst-case scenario" for each risk. It also includes information on the capabilities required to respond to and recover from the emergency, should the risk materialise. The NRR is based on the National Security Risk Assessment (NSRA), which is an internal, classified risk assessment that is used by the Government.[97]

78. Witnesses questioned how accessible the NRR was to organisations outside central government. Lord Harris described it as "a little bit too overwhelming" for small businesses and organisations,[98] while Cityforum argued that simpler language and concepts would make it more usable.[99]

79. A separate concern was whether the NRR adequately captures the relationships between different risks. Dr Maitland Hyslop wrote that the NRR "catalogues risks in silos" and that "this architecture underestimates the systemic nature of modern risk".[100] Rick Cudworth suggested that focusing on the common consequences of different risks would make guidance easier for businesses to understand and act upon.[101]

80. Witnesses also warned that excessive classification of risk and threat information hindered effective preparedness, limiting information sharing and making it harder for businesses to make informed investment decisions.[102]

Data sharing

81. We were told about problems with data sharing concerning vulnerable people. British Red Cross wrote that ineffective data sharing meant voluntary responders might not know which households and individuals most need humanitarian assistance.[103] Lieutenant General Sir Charles Stickland KCB OBE, Chair of Re:Act, said that data protection rules create silos in data usage.[104]

97 Cabinet Office, *National Risk Register 2026*
98 Q 34 (Lord Harris of Haringey)
99 Written evidence from Cityforum (NLR0149)
100 Written evidence from Dr Maitland Hyslop (NLR0013)
101 Q 14 (Rick Cudworth)
102 Written evidence from Professor David Alexander (NLR0006); National Gas (NLR0103); Offshore Energies UK (NLR0121)
103 Written evidence from British Red Cross (NLR0056)
104 Q 72 (Charles Stickland)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

82. Several suggestions were made to improve data sharing across organisations. Dr Carolyn Otley, Board Member of VCSEP, noted that data-sharing rules are already slightly more flexible during the response phase of a major incident, and suggested extending this flexibility to the preparedness and recovery phases as well.[105] Emily Morrison, Director of Sustainability at The Young Foundation, proposed bringing together existing data held by local authorities, consumer groups and others.[106] Citizens Advice advocated a Priority Services Register across energy, water and telecommunications providers to make it "less likely a consumer in vulnerable circumstances [would] fall through the cracks".[107]

83. Concerns extended beyond data on vulnerable people to the wider sharing of risk and threat information across organisations. The Security Institute said that "information relevant to risk, threat, and preparedness is often fragmented".[108] Polly Copeman, Senior Vice-President of Commercial Strategy and Operations at OpenHorizon, called for an "operational middle layer" to sit between the intelligence agencies and Critical National Infrastructure operators, translating threat information into decisions and practical action across sectors.[109] Ian Saunders suggested "an open-source National Resilience Insight Database" through which CNI operators, private companies and Government departments could identify, map and monitor unconventional threats in near real time.[110]

84. The Government highlighted steps it had taken to improve the sharing of sensitive information. The Cabinet Office said that the Government is sharing "more information" from the NSRA "than ever before".[111] Damian Johnson MBE, Director of Homeland Defence and Strategic Threats at the Ministry of Defence (MoD), told us that the MoD was reducing barriers for SME contractors by "allowing them access to more classified information".[112]

85. More broadly, the Cabinet Office said that since the establishment of the National Situation Centre, "data now leads responses by default", and that its Risk Vulnerability Tool enables it to "estimate the number of people who are vulnerable".[113] Zainab Agha, Director of Resilience and Recovery at the Ministry of Housing, Communities and Local Government, said: "Centrally, where we have information on vulnerabilities, we will share with local partners".[114] However, referring to the lack of data on vulnerable people during the pandemic, Dame Angela Eagle MP talked of a need to "get better at data and at contacts".[115]

86. **The National Risk Register places too much emphasis on individual risks and not enough on their consequences, limiting its usefulness for understanding and preparing for interconnected disruption.**

---

105 Q 72 (Dr Carolyn Otley)
106 Q 72 (Emily Morrison)
107 Written evidence from Citizens Advice (NLR0037)
108 Written evidence from the Security Institute (NLR0071)
109 Q 130 (Polly Copeman)
110 Written evidence from Ian Saunders (NLR0156)
111 Written evidence from the Cabinet Office (NLR0126)
112 Q 85 (Damian Johnson)
113 Written evidence from the Cabinet Office (NLR0126)
114 Q 181 (Zainab Agha)
115 Q 204 (Angela Eagle MP)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

87. **Effective resilience depends on timely information sharing. Data sharing remains too fragmented and inconsistent for a complex and fast-moving risk environment, risking vulnerable individuals and groups being inadequately informed and supported during an emergency.** This concern is not fully resolved by the Government's advice in its Be Ready campaign, which encourages vulnerable people to register for support from energy suppliers, network operators and water companies.

88. ***We recommend that the Government reflect the interdependent nature of many of the risks currently in the 2026 National Risk Register by consolidating these into a shorter list. It should give less emphasis in the National Risk Register to the causes of risks, and more to their consequences and how these can be mitigated.***

89. ***We recommend that the Government establish arrangements for sharing relevant and timely threat intelligence with designated, security-cleared personnel at critical national infrastructure operators. This should enable operators to better understand emerging threats, identify potential cascading impacts and take appropriate action to strengthen their resilience.***

Resilience planning

90. In 2025, the Government published its Resilience Action Plan.[116] Its key objectives are to:

- continuously assess how resilient the UK is to target interventions and resources effectively;
- enable the whole of society to take action to increase their resilience; and
- strengthen the core public sector resilience system.

91. Local Resilience Forums (LRFs), established under the Civil Contingencies Act 2004 and the Contingency Planning Regulations 2005, are multi-agency partnerships in England and Wales that bring together emergency services, local authorities, and the National Health Service (NHS) to prepare for major localised incidents. Their geographical areas are aligned with current police force boundaries.[117]

92. Witnesses highlighted gaps in co-ordination between national and local resilience structures, calling for closer alignment of the two.[118]

93. The evidence suggested that the Government's resilience strategies do not translate consistently into practical delivery. Professor Duncan Shaw and Dr Andrew McClelland said that the Plan does not fully articulate the role of national Government beyond legislation and policy.[119] The Local Government Association said that "it is not clear whether the cultural shift identified … is being achieved".[120]

116 Cabinet Office, *UK Government Resilience Action Plan*, 8 July 2025
117 Cabinet Office, *Local resilience forums: contact details*, 20 February 2023
118 Q 161 (Mark Williams); Q 3 (Matt Boughton)
119 Written evidence from Prof Duncan Shaw and Dr Andrew McClelland (NLR0026)
120 Written evidence from the Local Government Association (NLR0117)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

94. Witnesses raised concerns about the private sector's involvement in national resilience planning. ADS Group Ltd noted that, unlike the Strategic Defence Review, the National Security Strategy and Resilience Action Plan did not explicitly acknowledge industry's role.[121] Helena Coe said that awareness of the Resilience Action Plan remained "relatively low"[122], while Professor Ranger argued that unclear expectations were a barrier to action.[123]

95. Concern was expressed over how far communities are included in national plans. VCSEP wrote that "the Resilience Action Plan does not provide a shared framework for Voluntary, Community, and Faith sector (VCFS) action".[124] Emily Morrison similarly called for a national strategy for community resilience and a whole-society response.[125]

96. Witnesses highlighted that resilience arrangements should be more consistent across the UK, while remaining sufficiently flexible to reflect the different institutional and devolved structures of its constituent countries. Armagh City, Banbridge and Craigavon Borough Council reported that "national policies … are designed around structures that do not directly translate to the Northern Ireland context".[126] Simon Bradley proposed "formal equivalence boards" to ensure consistent national coverage while respecting devolved arrangements.[127]One problem raised was the complexity of the current system. Dr Hill told us: "We have a few too many different organisations looking at this". She suggested better use of existing structures rather than creating further organisations.[128]

97. We were told that the Government should be scrutinised over delivery of its plans by Parliament. The National Preparedness Commission said that "Parliament needs to have a continuing scrutiny role", suggesting a standing National Resilience Committee.[129] medConfidential wrote that "Parliament must have an institutional way of following up on recommendations", such as through the inclusion of these in departmental annual reports.[130]

Leadership

98. There was agreement among witnesses that strong leadership is essential to national resilience, but that it is lacking in the current system.[131]The National Fire Chiefs Council told us that "clear senior leadership with responsibility for cross-government resilience is a large gap in the current system".[132]

99. There were suggestions for an independent body to provide oversight and leadership. Stephen Arundell recommended an organisation modelled on the Office of Gas and Electricity Markets (Ofgem) that would identify best practice, set standards and audit performance.[133] Simon Boor suggested "a

121 Written evidence from ADS Group Ltd (NLR0040)
122 Q 11 (Helena Coe)
123 Q 136 (Prof Nicola Ranger)
124 Written evidence from the VCS Emergencies Partnership (NLR0151)
125 Q 77 (Emily Morrison)
126 Written evidence from Armagh City, Banbridge and Craigavon Borough Council (NLR0122)
127 Written evidence from Simon Bradley (NLR0142)
128 Q 47 (Fiona Hill)
129 Written evidence from the National Preparedness Commission (NLR0004)
130 Written evidence from medConfidential (NLR0023)
131 Q 38 (Fiona Hill); Written evidence from Cheong Lam (NLR0008); Dr Maitland Hyslop (NLR0013); National Fire Chiefs Council (NLR0055); The Security Institute (NLR0071)
132 Written evidence from the National Fire Chiefs Council (NLR0055)
133 Q 48 (Stephen Arundell)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

resilience body that is clearly distinct from the security apparatus, with its own public mandate and its own direct relationship with citizens".[134] Alex Woodman, National Lead for Resilience at the National Fire Chiefs Council, advocated a "national resilience forum" that could speak for the English Local Resilience Forums while preserving local delivery.[135]

100. The Scottish Government described a layered system in Scotland in which Regional and Local Resilience Partnerships bring together relevant responders, supported by national leadership.[136] The National Preparedness Commission suggested that this might be applied to England given "the announcement by the Home Office that police forces are to be merged".[137] Mark Williams commented that "a consideration of the LRF structure … will be very important".[138]

101. Witnesses highlighted the importance of clear decision-making responsibilities and command structures during crises. Polly Copeman suggested an operating model which would define "who is making the decisions, when and where".[139] Martin Frobisher, Group Safety and Engineering Director at Network Rail, described Network Rail's "bronze, silver and gold command structure", supplemented by a strategic crisis team for industry-wide incidents.[140]

102. The Cabinet Office provided evidence on the Government's future intentions. It said that decisions are taken to "build medium and long-term resilience and preparedness … informed by regular assessment and horizon scanning". It also said that the Government has "future plans to develop a common methodology to measure overall national resilience" and "will continue to provide regular updates on progress made to strengthen our resilience in an annual statement to Parliament".[141]

103. **The Government has not translated its whole-of-society ambition into consistent operational practice. Local Resilience Forums, the private sector, voluntary and community organisations, and bodies in the devolved administrations are still not included in forward planning early or consistently enough.**

104. **The Government seemed deficient in a clear command and control mechanism for translating top-down decision-making into lower-level delivery uniformly across the country.**

105. ***We recommend that the Government strengthen command and control between national (gold command) and local (bronze command) resilience structures before, during and after national emergencies. Developing middle-level (silver command) management, of the kind that exists in Scotland, should aim to translate national plans into local action, co-ordinate resources and volunteers, and oversee preparedness and performance. The***

134 Written evidence from Simon Boor (NLR0159)
135 Q 161 (Alex Woodman)
136 Written evidence from the Scottish Government (NLR0169)
137 Written evidence from the National Preparedness Commission (NLR0004)
138 Q 164 (Mark Williams)
139 Q 160 (Polly Copeman)
140 Q 154 (Martin Frobisher)
141 Written evidence from the Cabinet Office (NLR0126)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Government should establish regional co-ordination centres across the UK, using existing structures if possible.

Government structures

106. The Government operates a Lead Government Department (LGD) model for risks within the NSRA, whereby each risk is primarily owned and managed by the department with the main responsibility for the corresponding policy area. Where a crisis affects the whole system, the Cabinet Office takes responsibility for co-ordinating and overseeing the cross-government response and decision-making.[142] The Cabinet Office also provides the lead for newly identified or emerging risks that do not yet have a departmental lead.[143]

107. Resilience is within the portfolio of the Minister of State for Security, a role which spans both the Cabinet Office and the Home Office.[144] Resilience is also the focus of a sub-committee of the National Security Council (NSC), which is the Cabinet Committee that co-ordinates security strategy, defence policy, and intelligence operations. This ministerial committee is supported by an official-level structure in which Deputy National Security Advisers play a central co-ordinating role.[145]

108. Evidence offered qualified support for the LGD model. Paddy McGuinness, CMG OBE, former Deputy National Security Adviser for Intelligence, Security and Resilience, said that "you have to work through government departments" because they hold the relevant statutory powers.[146] Baroness Neville-Jones said that she had no better alternative to the LGD model because, under constitutional arrangements, "the money lies with the accountable Secretary of State".[147] Ed de Minckwitz said that "proper governance co-ordination and oversight above the Lead Government Department model" could make the system coherent.[148]

109. However, witnesses identified weaknesses in managing risks across departmental boundaries. Sian Jones warned that the involvement of multiple organisations meant that "things can slip through the cracks".[149] Baroness Neville-Jones said that departments have sometimes "omitted to take account of the interests of the other departments".[150] Jonathan Gray, Chief Underwriting Officer at Pool Re, told us about difficulties where issues "cut across multiple departments with differing priorities", adding that this was not resolved by the Cabinet Office's oversight.[151]

110. There was broad agreement among witnesses that resilience requires clear ministerial ownership.[152] Ian Saunders advocated for a more formal structure and said that there should be a "National Resilience Ministry with full

142 Cabinet Office, *UK Government Resilience Action Plan*, 8 July 2025
143 Cabinet Office, *SAGE Guidance*, 17 December 2024
144 Cabinet Office and Home Office, *Minister of State (Security Minister)*
145 Written evidence from the Cabinet Office to the House of Commons Science and Technology Committee, Cyber resilience of the UK's critical national infrastructure inquiry (CYB0039)
146 Q 190 (Paddy McGuinness)
147 Q 191 (Baroness Neville-Jones)
148 Q 190 (Ed de Minckwitz)
149 Q 3 (Sian Jones)
150 Q 191 (Baroness Neville-Jones)
151 Q 138 (Jonathan Gray)
152 Q 70 (Deborah Haynes); Q 70 (Elisabeth Braw); Q 191 (Baroness Neville-Jones); written evidence from Ian Saunders (NLR0156)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Cabinet-level representation, a ringfenced budget, and statutory responsibility for coordinating the UK's unconventional threat response".[153] Fiona Hill CBE stressed the importance of leadership from the Prime Minister, arguing that ministers could not deliver change at pace without their backing.[154] Witnesses also called for stronger oversight of national resilience, with the National Preparedness Commission proposing a Chief Resilience Officer at Permanent Secretary level.[155] Ed de Minckwitz suggested having "ministers in each department with resilience under their portfolio … convened twice a year".[156] Emerging Risks Global wrote that Finland "assigns preparedness duties to every ministry".[157]

111. We heard about greater ministerial responsibility for resilience adopted in other countries. HE Ambassador Kristina Beckvard of Denmark said that Denmark had established a Ministry of Resilience and Preparedness to "elevate and anchor the co-ordination and coherence of Danish activities to the highest political level".[158] HE Stefan Gullgren, Ambassador of Sweden, said that Sweden had appointed a Minister for Civil Defence "equally ranked to the Minister of Defence".[159]

112. The Government defended its current approach to allocating responsibility for national resilience. The Minister argued against appointing a minister solely responsible for resilience, on the basis that managing "interconnected risks is about how government works cross-departmentally and co-operatively up and down the system".[160] Similarly, the Cabinet Office emphasised that individual risks are owned by Lead Government Departments, whereas risks with significant cascading or whole-of-system impacts require co-ordination across government, since "one government department cannot be solely responsible for all mitigating actions".[161]

113. The Government described how the National Security Council sub-committee on Resilience operates. The Cabinet Office said that the Prime Minister had established it and that it was chaired by the Chancellor of the Duchy of Lancaster to make "collective decisions on our strategic choices".[162] The Minister said that the NSC "reports directly to the Prime Minister" and that the NSC sub-committee on Resilience could assemble relevant expertise for a crisis.[163]

114. **We were not convinced that Government structures concerning resilience are adequate to achieve the co-ordination required. The Lead Government Department model provides accountability and expertise but does not adequately address cross-departmental risks and competing priorities. Current ministerial arrangements also lack the seniority and capacity needed to provide sustained leadership and drive improvements with sufficient urgency.**

153 Written evidence from Ian Saunders (NLR0156)
154 Q 38 (Fiona Hill)
155 Q 9 (Mfon Akpan); written evidence from the National Preparedness Commission (NLR0004)
156 Q 191 (Ed de Minckwitz)
157 Written evidence from Emerging Risks Global (NLR0002)
158 Q 18 (Kristina Beckvard)
159 Q 18 (Stefan Gullgren)
160 Q 201 (Angela Eagle MP)
161 Written evidence from the Cabinet Office (NLR0126)
162 *Ibid.*
163 Q 202 (Angela Eagle MP)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

115. ***We recommend that within six months of publication of this report, the Government should appoint a cabinet minister responsible solely for resilience, who should chair the National Security Council Sub-Committee on Resilience. The Minister should be assisted by a Chief Resilience Officer at Permanent Secretary level. It should also appoint an official as Head of Preparedness in every department to support the Permanent Secretary on preparedness and security and co-ordinate preparedness within the department.***

116. ***We recommend that the Prime Minister make an annual statement to Parliament on the state of the UK's preparedness, setting out progress made in strengthening national resilience and outlining the Government's priorities for the year ahead.***

Legislation

Existing and proposed legislation

117. The Civil Contingencies Act 2004 provides the statutory framework for civil protection in the UK.[164] Under the Act, Category 1 responders—including emergency services, local authorities and NHS bodies—are the organisations at the core of most emergency responses and are subject to the full range of duties. These include risk assessment, emergency planning, business continuity, public warning and information, and co-operation and information-sharing with other responders. Category 2 responders, including transport and utility companies and the Health and Safety Executive, are bodies with more limited duties to co-operate and share relevant information with other responders.[165] The Government is required to review the Act's associated regulations every five years and has, in practice, also used these reviews to consider the Civil Contingencies Act 2004 as a whole. The next post-implementation review is due in 2027.[166]

118. Witnesses broadly supported the Civil Contingencies Act's statutory framework but raised concerns about its implementation and enforcement. Dräger described it as "a strong statutory foundation for planning, co-operation and information sharing", but reported inconsistent implementation.[167] The Local Government Association similarly highlighted difficulties in ensuring that some organisations, particularly utilities companies, took their statutory responsibilities seriously.[168] Alex Woodman told us that what is needed is not "heavy legislative change; it is government direction and policy advice".[169]

119. We also heard concerns about whether the distinction between Category 1 and Category 2 responders remains relevant. Bedfordshire Local Resilience Forum suggested that "the statutory duties of Category 2 responders should be strengthened".[170] Dr Nathan Hazlehurst said that "National Highways,

164 The Civil Contingencies Act (CCA) 2004 is supplemented by the CCA 2004 (Contingency Planning) Regulations 2005 (SI 2005/2042). The Regulations, and the CCA 2004 (Contingency Planning) (Scotland) Regulations 2005 (SI 2005/494) (the Scotland Regulations) which set out the duties on responders and specify in greater detail how they are to be performed.
165 Cabinet Office, *Preparation and planning for emergencies: responsibilities of responder agencies and others*, 20 February 2013
166 Cabinet Office, *Civil Contingencies Act 2004: Call for Views*, 14 July 2026
167 Written evidence from Dräger (NLR0052)
168 Written evidence from the Local Government Association (NLR0117)
169 Q 143 (Alex Woodman)
170 Written evidence from Bedfordshire Local Resilience Forum (NLR0130)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Network Rail and Transport for London are Category 2 responders, yet provide a first responder capability".[171]

120. Witnesses also identified shortcomings in the Act's treatment of voluntary and community organisations. VCSEP said that engagement with the sector was encouraged rather than required, resulting in inconsistent practice between LRFs.[172] The British Red Cross viewed the planned 2027 review as an opportunity to strengthen the sector's integration into resilience arrangements.[173]

121. The Government provided evidence on its approach. The Minister said that Part 1 of the Civil Contingencies Act "is solid and works well" and that the upcoming review of it might address changes to LRF boundaries and English devolution.[174] Roger Hargreaves, Director of the Civil Contingencies Secretariat, characterised the review as being as much about regulations, guidance and delivery as changing the primary legislation itself.[175] The Cyber Security and Resilience (Network and Information Systems) Bill, introduced on 12 November 2025, would extend cyber security requirements to more organisations and strengthen incident reporting, information sharing and enforcement. It would also give the Secretary of State powers to set strategic priorities and direct regulators or regulated entities in response to national security threats.[176]

122. Witnesses raised concerns about the scope and ambition of the Cyber Security and Resilience Bill. Baroness Neville-Jones expressed concern that it did not go far enough in providing for wider private-sector involvement and partnership.[177] Paddy McGuinness suggested it was a combination of disparate measures and thought it was not adequate to address the severity of cyber threats.[178] Particular concern focused on organisations and sectors that would remain outside the Bill's regulatory scope. ISACA wrote that "large parts of the economy … will remain outside [the] regulatory perimeter", calling for measures concerning organisations which could create systemic problems if they malfunction.[179] ISC2 highlighted the broader scope of the EU's Network and Information Systems 2 (NIS2) Directive, noting that, unlike the Cyber Security and Resilience Bill, it includes manufacturing, public administration and food production within its remit. It also said that businesses outside the Bill's regulatory scope, including SMEs, needed additional measures through the National Cyber Action Plan to improve cyber resilience.[180]

123. ISC2 also highlighted the need for greater alignment of cybersecurity requirements across jurisdictions, warning that differing standards and reporting obligations could impose unnecessary compliance burdens on organisations operating internationally.[181]

---

171 Written evidence from Dr Nathan Hazlehurst (NLR0012)
172 Written evidence from the VCS Emergencies Partnership (NLR0151)
173 Written evidence from British Red Cross (NLR0056)
174 Q 212 (Angela Eagle MP)
175 Q 212 (Roger Hargreaves)
176 Department for Science, Innovation and Technology, *Cyber Security and Resilience (Network and Information Systems) Bill: factsheets—Summary of the Bill* (12 November 2025)
177 Q 199 (Baroness Neville-Jones)
178 Q 199 (Paddy McGuinness)
179 Written evidence from ISACA (NLR0133)
180 Written evidence from ISC2 (NLR0050)
181 *Ibid.*

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

124. Witnesses raised concerns about how the Bill would be enforced in practice. Ed de Minckwitz noted that although it requires organisations to develop plans, "there is nothing to mandate that they are tested".[182] Vsevolod Shabad suggested that the Bill should "require designated oversight bodies … to demonstrate … cyber security governance capacity over the bodies they oversee".[183]

125. Artificial intelligence poses a strategic challenge to national resilience by increasing the scale and sophistication of cyber threats, exacerbating every threat, accelerating the spread of disinformation, and introducing new vulnerabilities within critical national infrastructure. Effective governance and regulation are essential to ensure that AI enhances, rather than undermines, security, public trust, and societal resilience.[184]

Future legislation

126. The National Preparedness Commission and ADS Group Ltd called for the Defence Readiness Bill to be introduced without delay, with the Commission proposing that it be enacted in 2027.[185]

127. Witnesses also proposed legislation to address specific resilience vulnerabilities. Professor Lang told us that "we need a new Food Security and Resilience Act" providing durable strategic direction for the whole food system.[186] Edward Lucas, Senior Fellow at the Centre for European Policy Analysis, said that "we need legislation to keep dirty money … out of our political system" in the context of legal intimidation, opaque political finance, and hostile-state influence.[187] The 2026 King's Speech announced several legislative measures relevant to national resilience. The Armed Forces Bill would expand the pool of reservists available for recall, while the Tackling State Threats Bill would provide new powers to disrupt organisations linked to hostile-state activity. Wider measures included an Energy Independence Bill intended to strengthen energy security and a Clean Water Bill providing for statutory resilience standards, asset mapping and longer-term planning in the water sector.[188]

128. Some witnesses supported stronger statutory duties for private sector organisations. Professor Ranger said that "there is nothing in current legislation … that incentivises a company to do things in the national interest", suggesting more widespread scenario analysis as performed in the financial sector.[189] Baroness Neville-Jones suggested that legal obligations could help businesses justify investment in resilience.[190] Other evidence called for clearer statutory expectations around resilience, business continuity and reporting.[191]

---

182 Q 197 (Ed de Minckwitz)
183 Written evidence from Vsevolod Shabad (NLR0079)
184 Written evidence from Escode (NLR0113)
185 Written evidence from the National Preparedness Commission (NLR0004); written evidence from ADS Group Ltd (NLR0040)
186 Q 117 (Prof Tim Lang)
187 Q 68 (Edward Lucas)
188 UK Government, *The King's Speech 2026: background briefing notes*, 13 May 2026
189 Q 138 (Prof Nicola Ranger)
190 Q 199 (Baroness Neville-Jones)
191 Written evidence from SafehousePro UK Ltd (NLR0030); National Fire Chiefs Council (NLR0055); Resilient Cities Network (NLR0099)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

129. However, witnesses also cautioned against relying too heavily on regulation. Helena Coe said that "regulatory compliance should not be seen as the be-all and end-all" because this would not guarantee genuine resilience.[192] Rick Cudworth said: "We should not regulate small businesses across the board", adding that regulation of larger businesses might lead them to increase requirements on SMEs within their supply chains.[193]

130. Questions were raised about whether the current statutory footing of Local Resilience Forums is sufficient. Mark Williams talked of the need for this given that the LRF system is "the building block for whole of society resilience".[194] Bedfordshire Local Resilience Forum said that a "lack of statutory status significantly limits our ability to hold partners to account".[195]

131. We were told about the Government's approach to future legislation. Margaret Read, Strategy and Policy Director at the National Infrastructure and Service Transformation Authority (NISTA), said that measures in the Clean Water Bill would extend existing resilience requirements to certain third parties.[196] Damian Johnson told us that the Defence Readiness Bill might address mobilisation of industry and reserves, access to CNI and resources, war-fighting infrastructure and NATO host-nation support. He added that "you would expect us to take our time on that"[197] and that "we will not legislate just for the sake of it".[198]

132. **Artificial intelligence presents a further challenge to national resilience, amplifying existing threats and creating new vulnerabilities. Effective governance and regulation are essential to manage these risks and harness its potential benefits.**

133. **The Government's legislative programme is not keeping pace with the resilience challenges identified by this inquiry. The Civil Contingencies Act 2004 provides a statutory framework, but Category 2 responders do not always engage as required. The Cyber Security and Resilience (Network and Information Systems) Bill would provide useful baseline requirements, but its scope is limited, while the Defence Readiness Bill has been delayed despite the importance of its subject matter.**

134. ***We recommend that the Government remove the distinction under the Civil Contingencies Act 2004 between Category 1 and Category 2 responders, giving all of them the responsibilities of current Category 1 responders. It should change the wording that "encourages" engagement with wording that "requires" engagement with the Voluntary, Community and Faith Sector and the private sector.***

135. ***We recommend that the Government widen the scope of cyber security regulation beyond the provisions of the Cyber Security and Resilience (Network and Information Systems) Bill, ensuring that regulators have sufficient resources and capacity to enforce requirements effectively. It should also keep the regulatory***

192 Q 13 (Helena Coe)
193 Q 13 (Rick Cudworth)
194 Q 143 (Mark Williams)
195 Written evidence from Bedfordshire Local Resilience Forum (NLR0130)
196 Q 131 (Margaret Read)
197 Q 89 (Damian Johnson)
198 Q 91 (Damian Johnson)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

framework under continuous review and update it regularly to reflect evolving cyber threats and technological developments.

136. ***We recommend that the Government bring forward the Defence Readiness Bill as a matter of urgency to establish clear statutory responsibilities for national resilience across society. The Bill should place Local Resilience Forums on a statutory footing, with clear command and control status, provide for sustainable funding and strengthen accountability for preparedness at national and local levels.***

International frameworks

137. As a member of the North Atlantic Treaty Organisation (NATO), the UK is committed under Article 3 of the Treaty to maintain and develop its capacity to resist armed attack. At the 2016 NATO Summit, leaders of the Allies agreed seven baseline requirements for national resilience: continuity of Government and critical Government services, resilient energy supplies, ability to deal with uncontrolled movement of people, resilient food and water resources, ability to deal with mass casualties and disruptive health crises, resilient civil communications systems, and resilient transport systems.[199]

138. Witnesses told us that the NATO baseline requirements had not visibly reached the contracts, services and practitioners that would have to deliver them. Dr Hugh Deeming warned that road network contracts rarely reflected these requirements,[200] and Dr Gogalniceanu said that frontline clinicians may be unaware of NATO medical requirements.[201] The International Association for Resilience Analysis said that "the degree to which NATO resilience benchmarks inform domestic policy, or are visible to Parliament, remains unclear".[202]

139. Witnesses also suggested ways to translate NATO's baseline requirements more effectively into domestic practice. Bittium recommended "mandating NATO-aligned interoperability standards" so that UK defence, civilian infrastructure and industry could operate together and with allies under disruption.[203] The International Association for Resilience Analysis called for the Government to publish UK performance against all seven NATO civil preparedness baselines and incorporate identified gaps into a national resilience assessment.[204]

140. We heard that EU regulatory frameworks could provide useful models for strengthening UK resilience. CogitoPraxis Nederland BV said that UK resilience would be enhanced by the adoption of provisions similar to those in the Critical Entities Resilience (CER) Directive, which sets resilience requirements for designated critical entities.[205]

141. Evidence also highlighted wider international frameworks relevant to disaster risk reduction and the resilience of cross-border infrastructure. Byatt described the Sendai Framework for Disaster Risk Reduction 2015–

199 NATO, *Resilience, civil preparedness and Article 3*, 18 September 2026
200 Written evidence from Dr Hugh Deeming (NLR0160)
201 Q 149 (Dr Peter Gogalniceanu)
202 Written evidence from the International Association for Resilience Analysis (NLR0066)
203 Written evidence from Bittium (NLR0116)
204 Written evidence from the International Association for Resilience Analysis (NLR0066)
205 Written evidence from CogitoPraxis Nederland BV (NLR0039)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

2030[206] as "a global framework for all nations to use" and suggested that the UK could work with the UN Office for Disaster Risk Reduction to lead or co-lead its post-2030 revision.[207] Viasat UK highlighted the importance of internationally agreed rules governing satellite services, on which many of the UK's vital services and critical infrastructure depend. It said that "globally agreed rules, decided by all nations at the International Telecommunication Union (ITU)", have enabled the growth of satellite services.[208]

142. The Security Minister said that recent NATO agreements required the UK to become "much more resilient in the homeland as well as in a military sense", and that the Government was "preparing to do a lot more".[209] Damian Johnson said that the Government's planned Home Defence Programme was designed to strengthen national resilience "in line with our NATO Article 3 commitment".[210] Lt-Gen Griffiths described the military's Fortitude programme, which translates NATO baseline commitments into operational planning.[211]

143. **The Government has not demonstrated that the UK currently meets its NATO civil preparedness commitments in practice. We received no clear evidence showing the extent to which the seven baseline requirements are met, how compliance is assessed, or how gaps are addressed. This lack of transparency prevents effective parliamentary scrutiny of the UK's preparedness against commitments it has undertaken.**

144. ***We recommend that the Government publish UK performance against all seven NATO civil preparedness baselines and explain the improvements that will be made where requirements have not been met. It should monitor international frameworks on resilience, particularly EU legislation and directives, and apply these in the UK where relevant.***

206 UN Office for Disaster Risk Reduction, *Sendai Framework for Disaster Risk Reduction 2015–2030*
207 Written evidence from Gareth Byatt (NLR0104)
208 Written evidence from Viasat UK (NLR0132). See also written evidence from the Future Resilience Forum (NLR0147) and UK Defence First (NLR0019).
209 Q 203 (Angela Eagle MP)
210 Q 78 (Damian Johnson)
211 Q 78 (Paul Griffiths)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

CHAPTER 4: ACTIVATING THE WHOLE OF SOCIETY

145. If national resilience is everyone's responsibility, does everyone know what role they are expected to play and are they equipped to deliver it? This chapter considers whether the UK has moved beyond the ambition of a whole-of-society approach by giving Government, businesses, communities and individuals clear responsibilities and the capability to fulfil them.

Who has a role to play?

146. With a population of around 70 million, embedding resilience across the UK is a significant challenge. A consistent theme across the evidence we received was that resilience should not be treated as a discrete emergency planning function, but as a core, cross-cutting principle embedded across Government policy, planning and decision-making.[212] This should encompass security, civil protection and defence, economic continuity, infrastructure resilience, democratic legitimacy and social cohesion, reflecting the broad approach taken in Finland's comprehensive security model.

147. The British public has demonstrated a willingness to contribute during emergencies. During the COVID-19 pandemic, 750,000 people signed up as NHS Volunteer Responders within four days of the scheme opening, three times the number the Government had asked for, while thousands of local mutual aid groups formed to deliver food and medicine and to check on isolated and vulnerable neighbours.[213] Pupils 2 Parliament similarly found that the students it consulted believed young people should have a role in preparing for and responding to emergencies.[214] This is supported by our own survey of young people (see Appendix 6).

148. Willingness, however, is not the same as preparedness. The Government's 2026 public survey found that 50% of respondents felt their household was only slightly or not at all prepared for an emergency, and 54% considered themselves poorly informed about national emergency plans.[215] We heard that giving people clear, honest information, practical guidance and a defined role is what will turn goodwill into genuine preparedness.[216]

149. Societal preparedness was also identified as an important part of national resilience, helping to reduce vulnerability and strengthen the country's ability to withstand disruption.[217] Stephen Arundell told us that stronger societal preparedness meant "there is less ask of the state"[218], while Simon Boor described resilience as "a form of deterrence" arguing that a country able to absorb disruption and maintain continuity is harder to destabilise.[219] NATO identifies "assured continuity of government and critical government services" as the first of its seven baseline requirements for national resilience, rooted in Article 3 of the North Atlantic Treaty.[220]

212 Written evidence from the Institute of Civil Protection and Emergency Management (NLR0096); The Security Institute (NLR0071); Brave Within LLP (NLR0067)
213 NHS England, *NHS army of volunteers to start protecting vulnerable from coronavirus in England*, 7 April 2020; Q 139 (Matt Killick BEM); written evidence from Prof John Drury (NLR0025)
214 Written evidence from Pupils 2 Parliament (NLR0165)
215 Cabinet Office, *UK Public Survey of Risk Perception, Resilience and Preparedness 2026*, 19 August 2026
216 Q 93 (Sam Wise)
217 Written evidence from the Chartered Institution of Highways & Transportation (NLR0084); National Preparedness Commission (NLR0004); Bryon Hyde (NLR0070)
218 Q 52 (Stephen Arundell)
219 Written evidence from Simon Boor (NLR0007)
220 NATO, *Resilience, civil preparedness and Article 3*, 18 September 2026

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

150. Evidence identified a gap between awareness and practical preparedness. SafehousePro told us that "The UK does not face a deficit of concern about risk, but a deficit of practical, accessible pathways to preparedness".[221] One witness explained that the issue is about "joining the dots" and filling in the gaps, "not reinventing the wheel".[222]

151. **The public, including young people, has demonstrated a strong willingness to contribute during national emergencies, but this has not yet been translated into consistent levels of preparedness. The evidence shows that resilience depends on turning willingness, plans and institutional responsibilities into coordinated capability across Government and wider society. This requires clear roles, practical skills and arrangements that work together in practice.**

152. **Politicians and officials need to trust the public and take them into their confidence as much as security will allow, while offering them opportunities to play a fuller role as active citizens in response and recovery. The Government's Be Ready campaign marks a welcome step in this direction, but sustained, serious and measured communication from political leaders will be essential to building public confidence.**

Vision and plans

153. To date, the Government has conveyed its top-down plans through the 2025 UK Resilience Action Plan. Objective 2 of the plan is titled 'Enable the whole of society to take action to increase their resilience'.[223] It describes five actions that the Government aims to implement:

- ask and support the public to take action;
- better integrate services from voluntary, community and faith services;
- improve the resilience of Critical National Infrastructure;
- provide the right tools to work with the private sector; and
- bring together organisations.[224]

154. The evidence we received questioned whether, by themselves, these aims provide the specificity required of a national resilience plan. Witnesses pointed in particular to the absence of sufficiently clear roles, measurable expectations and an overall account of what capability is required, at what scale and by when.[225]

155. Evidence highlighted the need to bridge the gap between national resilience policy and the capabilities that exist across wider society. SafehousePro told us that a whole-of-society approach "cannot be legislated into existence from above" but must be "operationalised from below", embedding practical capability across society.[226]

221 Written evidence from SafehousePro UK Ltd (NLR0030)
222 Q 45 (Stephen Arundell); Q 75 (Emily Morrison)
223 Cabinet Office, *UK Government Resilience Action Plan*, 8 July 2025, para 11
224 *Ibid.*
225 Q 136 (Professor Nicola Ranger); written evidence from the National Preparedness Commission (NLR0004); Prof Duncan Shaw; Dr Andrew McClelland (NLR0026); International Association for Resilience Analysis (NLR0066)
226 Written evidence from SafehousePro UK Ltd (NLR0030)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Box 2: International case studies

Several countries in Europe and Asia treat national resilience as a whole-of-society responsibility. Norway's Ambassador, HE Tore Hattrem, told us that the Nordic approach does not "separate private industry, civil society, independent institutions and defence", because "everybody must play their role".[227]

Finland provides a particularly developed example. HE Teemu Turunen told us that "the cornerstone of our preparedness lies in civil society preparedness", with businesses and individual citizens expected to understand their roles.[228] This is supported by national defence courses, extensive civil-defence infrastructure and arrangements for security of supply involving Government and business. HE Teemu Turunen also linked preparedness directly to deterrence: "The more prepared we are, the less our neighbour will have an appetite for coming after us".[229]

Sweden similarly combines military and civil preparedness. HE Stefan Gullgren described resilience in terms of "awareness of risk, readiness to act and trust in institutions".[230] Sweden's Total Defence Duty Act also provides for residents aged 16 to 70 to undertake civil-defence functions when required.[231] Norway designated 2026 its "Total Defence year", with municipalities, businesses and citizens encouraged to strengthen their preparedness for crisis and war.[232]

Emerging Risks Global described Singapore's Total Defence framework as "the most explicitly codified whole-of-society model in the Indo-Pacific", encompassing military, civil, economic, social, psychological and digital defence.[233] Evidence also highlighted the efforts of Japan, Germany and the Netherlands, including Japan's integration of preparedness into education and local community planning.[234]

156. Evidence showed that the UK is not starting from scratch when it comes to resilience planning. Existing networks, institutions and community structures could provide much of the infrastructure for a whole-of-society approach. One submission stated that "the most practical entry point for building whole-of-society resilience in rural Britain already exists" pointing to farming networks, community organisations, river stewardship projects and younger farmers in areas such as Pembrokeshire.[235]

157. Local authorities were considered to play an important role in co-ordinating resilience efforts at the local level. There was evidence that local preparedness programmes could be designed with the involvement of councils[236], and that parish and town councils should be consulted as a mandatory part of future resilience planning.[237]

158. We heard that the Government has taken steps to strengthen civil society's role in resilience. Jonathan Martin, Director for Project Delivery and Major

227 Q 18 and Q 26 (Tore Hattrem)
228 Q 18 and Q 24 (Teemu Turunen)
229 Q 23 (Teemu Turunen)
230 Q 18 (Stefan Gullgren)
231 Q 24 (Stefan Gullgren)
232 Written evidence from Tore Hattrem (NLR0011)
233 Written evidence from Emerging Risks Global (NLR0002)
234 Written evidence from the National Emergencies Trust (NLR0114); Dr Dolapo Fakuade and Dr Justin Okoli (NLR0127)
235 Written evidence from Sazani Associates (NLR0021)
236 Written evidence from SafehousePro UK Ltd (NLR0030)
237 Written evidence from the National Association of Local Councils (NLR0041)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Events at the Department for Culture, Media and Sport, told us that the Civil Society Resilience Infrastructure Fund would enable civil society organisations to "share views and insights and collaborate with government on resilience", while strengthening knowledge and relationships across the sector.[238] The Fund aims to strengthen civil society's "knowledge, skills, relationships and capabilities".[239] Witnesses emphasised, however, that this capability requires sustained support. VCSEP called for "flexible, long-term investment",[240] while Matt Killick argued that the voluntary sector needs to provide "a standing capability and capacity" rather than remain "more of an emergency add-on".[241]

159. **While we welcome the action taken by the Government through its Be Ready campaign to improve public preparedness, we conclude that its other aims under Objective 2 of the 2025 Resilience Action Plan remain vague and fail to establish clear responsibilities for delivery. We are concerned that activity under the Plan is being treated as progress without evidence that the country is better prepared.**

160. **The UK does not need to build its whole-of-society capability from scratch. Existing local authorities, community organisations, cultural institutions and voluntary groups already provide much of the infrastructure needed. The problem is that this capability is not yet consistently recognised or integrated into the national resilience system, nor is it supported by statutory arrangements or sustained funding. Civil society remains too often an emergency add-on, rather than a standing national capability.**

Delegating Responsibility

161. Effective resilience requires communities and local organisations to have the authority and capability to take decisions and act in response to local needs, without transferring responsibility away from the state.[242] The Niinisto Report (2024) for the EU said that to "empower citizens [was] the backbone of societal resilience and preparedness".[243] Such empowerment is particularly important where statutory responders may not be immediately available.[244]

162. Professor Duncan Shaw and Dr Andrew McClelland told us that many local resilience partnerships were piloting Community Emergency Hubs to support local preparedness[245] An example of this approach was provided by 'How Resilient is Cambridge' (HRC), a series of public meetings which brought together local and national experts, community groups, local councillors and members of the public to consider issues including food, flooding, energy and communications.[246] The initiative attracted 420 bookings and generated specific actions for local councillors. Resilience Web CIC told us that HRC had already produced tangible outcomes: "there have been changes made to

238 Q 181 (Jonathan Martin)
239 DCMS, *The Civil Society Resilience Infrastructure Fund: application guidance*, 1 May 2026
240 Written evidence from the VCS Emergencies Partnership (NLR0061)
241 Q 147 (Matt Killick)
242 Written evidence from Anna Goodden, Dr James Porter and Dr Francesca Vantaggiato (NLR0062)
243 European Commission, *Strengthening Europe's Civilian and Military Preparedness and Readiness*, 2024, pp 19–21
244 Written evidence from Safehouse Pro UK Ltd (NLR0030); National Fire Chiefs Council (NLR0055)
245 Written evidence from Prof Duncan Shaw, Dr Andrew McClelland (NLR0026)
246 Written evidence from Resilience Web, CIC, Cambridge Room (NLR0074)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

the draft Local Plan for Cambridge to add a section on food security".[247] It also reported that discussions had begun on changing local rules to enable greater repair and reuse of electronic items.

163. Dame Angela Eagle MP said that:

> "We need to enable and empower [a national response] to happen. We do not need to try to control it all from the top or the centre. If we can get better at data and at contacts, and if we can empower the local resilience forums so that they can take more of the kind of initiatives that happened spontaneously during COVID-19, that is all to the good."[248]

164. We heard that the Government is testing greater local leadership through its Stronger LRF Trailblazers programme.[249] Five of England's 38 Local Resilience Forums are participating in the programme, with £2.5 million provided to test how they can strengthen their approach and become "proactive locally about building resilience".[250] The Security Minister said that lessons from the programme would inform the forthcoming review of the Civil Contingencies Act.[251]

165. ***We recommend that the Government should make local empowerment a central principle of its resilience approach. It should go beyond the Be Ready campaign and take active measures to support communities and businesses in their resilience preparations by enabling decisions to be taken at the lowest appropriate level within a clear national strategy and shared objectives.***

166. ***We recommend that the Government review whether existing Local Resilience Forums in England and Wales, Regional Resilience Partnerships in Scotland, and Emergency Preparedness Groups in Northern Ireland provide sufficient coverage to support whole-of-society resilience at community level. It should work with local authorities, involving community organisations, to ensure that the support needed for people who are vulnerable for a variety of reasons is available.***

The Role of the Private Sector

167. We heard that the private sector has a wider role in national resilience than its statutory responsibilities under the Civil Contingencies Act 2004, including those applying to Category 2 responders and operators of Critical National Infrastructure. Ian Saunders told us that "over 80% of the UK's CNI is privately owned and maintained",[252] while Rick Cudworth argued that Government was "missing out a complete layer, which is business" in its approach to resilience.[253] The Resilience Action Plan itself recognises that national resilience extends beyond formally designated CNI to "wider essential services".[254]

247 *Ibid.*
248 Q 204 (Angela Eagle MP)
249 Written evidence from the Cabinet Office (NLR0126)
250 Q 204 (Angela Eagle MP)
251 *Ibid.*
252 Written evidence from Ian Saunders (NLR0156)
253 Q 12 (Rick Cudworth)
254 Cabinet Office, *UK Government Resilience Action Plan*, 8 July 2025, para 63

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

168. Evidence highlighted the growing exposure of businesses to interconnected risks. Professor Ranger explained that environmental risks, including extreme weather, were increasingly compounding other shocks, such as geopolitical disruption affecting global supply chains and energy costs.[255] Rick Cudworth warned that these risks could be "potentially existential" for businesses.[256] Business in the Community emphasised that the private sector was not a homogeneous group, and that expectations should reflect differences in business size, sector and capacity.[257]

169. SMEs were identified as particularly vulnerable, given their importance within critical supply chains. The Association of British Insurers (ABI) reported that its members paid out £197 million to help businesses recover from cyber incidents in 2024, an increase of 230% on the previous year. It warned that smaller businesses may underestimate their exposure to cyberattacks and that Government data shows that 50% of UK SMEs faced a cyberattack in 2025.[258] Howden cited research which found that "60% of SMEs without cyber cover go bankrupt within six months of a severe incident".[259]

170. Insurance is one way in which companies can mitigate the risk of acute incidents as it helps protect from events occurring and pay claims post-event. The industry said:

> "The take up of cyber insurance and terrorism cover by SMEs in the UK is very low … leaving the majority at risk of significant losses in the event of an attack. To increase the resilience across the UK economy, increasing the proportion of SMEs purchasing terrorism and cyber insurance is critical."[260]

171. Oliver Neuberger of Accenture described cyber insurance as a "financial mitigation mechanism" but cautioned that it cannot protect against losses such as "reputational damage" and "indirect losses".[261] He said its greater resilience value lay in "those standards that cyber insurers will mandate", including incident-response arrangements and security controls.[262]

172. Witnesses warned that commercial pressures and a focus on cost-efficiency could discourage investment in resilience. Helena Coe said that narrow margins could prevent businesses from addressing supply-chain vulnerabilities, while the Society of Chemical Industry and Sandoz highlighted the risks of reliance on imported goods and procurement practices that prioritise price. Edward Lucas described moving from "just-in-time" to "just-in-case" stockholding as "expensive, but it is a kind of insurance".[263]

173. Public-private insurance arrangements also have a role in supporting wider national resilience. These traditionally apply when the risk is too great for the insurance market to bear on its own, or when the cost is prohibitive to companies. Flood Re, a government-backed reinsurance scheme, was

255 Q 125 (Prof Nicola Ranger)
256 Q 10 (Rick Cudworth)
257 Written evidence from Business in the Community (NLR0166)
258 Written evidence from the Association of British Insurers (NLR0129)
259 Written evidence from Howden (NLR0044)
260 Written evidence from the ABI (NLR0129). Quoted according to PoolRe.
261 Q 56 (Oliver Neuberger)
262 *Ibid.*
263 Q 69 (Edward Lucas)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

established to help households in flood-risk areas access affordable insurance. The scheme is due to end in 2039, although the Government is reviewing whether this remains appropriate in light of climate change.[264]

174. Witnesses emphasised the importance of closer co-operation between government and businesses. Baroness Neville-Jones was clear that: "You have to bring the private sector in. Resilience is a partnership issue. The private sector needs to be in there early."[265] Rick Cudworth said that: "Government and business both have a shared interest in a safe, stable and investable UK, which is a key element of resilience."[266]

175. In October 2026, Defra expanded its Floods Resilience Taskforce to include drought resilience, bringing together government, industry and community representatives to improve preparedness for extreme weather and support a more co-ordinated approach to managing flood and drought risks.[267] We look forward to seeing what its powers and terms of references are and the speed at which it will report.

176. One submission argued that the role of essential businesses in national resilience is insufficiently defined, with unclear and non-mandatory expectations creating a risk of confusion and inaction.[268] In Sweden, essential businesses are designated 'K' companies, Elisabeth Braw told us that these companies are identified in advance, with Government subsidies available to support the additional cost of preparedness.[269] Finland provides an example of a more differentiated approach to business resilience. Its security-of-supply system combines statutory requirements for certain critical operators, contractual arrangements to safeguard the continuity of essential services, and voluntary preparedness by the wider business community (See appendix 7).[270] This allows the level of obligation to reflect the role and criticality of different businesses, rather than applying the same requirements across the private sector.

177. The Minister distinguished between the engagement required for SMEs, large firms and regulated critical infrastructure, and gave an example of roundtables through which agricultural suppliers provided detailed information on supply-chain risks.[271] The Minister added that the Government currently preferred voluntary business action to the imposition of statutory duties.[272]

178. **The private sector is not adequately integrated into national and local resilience planning. Businesses operate most of the infrastructure, logistics and supply chains on which the country depends, but their representation within resilience structures has been inconsistent or ignored.**

264 HC Written Answer, 11120, Session 2024–26
265 Q 191 (Baroness Neville-Jones)
266 Q 12 (Rick Cudworth)
267 Department for Environment, Food and Rural Affairs, *New taskforce to boost Britain's resilience to flooding and drought*, 11 October 2026
268 Written evidence from Róisín Jordan; Prof Duncan Shaw; Dr Andrew McClelland (NLR0033)
269 Q 62 (Elisabeth Braw)
270 Finnish National Emergency Supply Agency, *Methods and tools*
271 Q 205 (Angela Eagle MP)
272 Q 207 (Angela Eagle MP)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

179. ***We recommend that the Government establish a tiered framework for business resilience, proportionate to the criticality, size and risk profile of organisations. Tier 1 should be for businesses whose continued operation is essential to national resilience, which should be subject to statutory preparedness and continuity duties and regular stress tests. Tier 2 should be for organisations for whom statutory duties are not necessary, where the Government should use contractual arrangements to set and assure appropriate resilience requirements. Tier 3 should be for the wider business community, including SMEs, whose preparedness should be supported through voluntary, practical and sector-specific guidance, incentives such as tax reliefs and cheaper insurance for compliant businesses and opportunities to participate in resilience planning and exercising. The Government should clearly define which businesses fall within each tier and what is expected of them.***

180. ***We recommend that the Government ensure that businesses of all sizes and public authorities recognise cyberattacks as a significant risk to their operations and take appropriate steps to strengthen their resilience. This should include promoting greater awareness of cyber risks and the role that insurance can play in mitigating their financial consequences, alongside practical measures to prevent, withstand and recover from attacks.***

181. ***We recommend that the Government ensure that Flood Re, a world first reinsurance scheme providing homeowners with affordable insurance, is extended beyond its planned end date of 2039. It should adapt public-private reinsurance models to provide more effective cover for risks that are difficult to insure, including large-scale cyber-attacks.***

Education and Training

182. There was consensus among witnesses that preparedness and resilience should be taught from an early age. The British Red Cross similarly argued that resilience education should provide "practical, actionable skills", including crisis decision-making and first aid, and be incorporated into the curriculum to ensure "consistent access for young people across the board".[273]

183. On 4 June 2026 we held a roundtable with 20 university students from across the United Kingdom (see Appendix 6). Participants suggested that preparedness should begin earlier in life, and saw schools, universities and local authorities as useful routes for teaching practical skills and explaining local risks. They highlighted first aid, cardiopulmonary resuscitation (CPR), survival skills and household emergency planning, alongside education on climate and flood risks, digital safety, critical thinking and how to identify reliable information. Some said that even basic skills of this kind had not been taught consistently at school. This was echoed by evidence from Pupils 2 Parliament: 72% of those consulted said that schools did not teach enough about dealing with emergencies, with pupils calling for teaching to cover not only what emergencies are, but what to do when they occur.[274]

273 Written evidence from British Red Cross (NLR0056)
274 Written evidence from Pupils 2 Parliament (NLR0165)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

184. We also heard about ways of involving young people more directly in national resilience and defence. Lieutenant General Sir Charles Collins said that, while the Government was not pursuing the kind of total-defence model used in Finland, there was scope for a broader form of reserve service, and described the cadet movement as "a great way of embedding resilience into society".[275] Lieutenant General Paul Griffiths told us that military commanders were developing the Government's proposed Armed Forces "Gap Year" Foundation Scheme, modelled on the Australian scheme, which the Army intended to begin in September 2026.[276] The Royal Navy and the Royal Air Force are also expected to participate and the MOD has allocated £13 million to deliver the initial pilot.[277] Similar approaches are being developed elsewhere in Europe. France introduced a voluntary ten-month national service for 18 to 25-year-olds in September 2026, intended in part to strengthen national resilience and the connection between young people and the armed forces.[278]

185. The evidence also pointed to the contribution that older people could make to national resilience. SafehousePro argued that people aged 55–70 represent a "substantial and largely untapped asset" for national resilience, bringing "deep local knowledge", established community relationships and professional experience.[279] It proposed a national resilience volunteering programme for this group, which could "address workforce capacity gaps in community resilience" while reducing social isolation and recognising "the real contribution this group can make".[280] Evidence from Northern Ireland also highlighted the value of intergenerational approaches in building long-term community resilience.[281]

186. This life-course approach was reflected in Simon Bradley's proposed Societal Training and Enhanced Preparedness Upskilling Programme (STEP-UP).[282] The programme starts in pre-school (ages 3–5) then moves through ages 5–16 in schools (by enhancing the PSHE and Citizenship parts of the National Curriculum) before advancing to community first responders and then retirees (65+).

187. The UK Resilience Academy (UKRA) provides training and professional development for those responsible for resilience across the UK. Dr Eleanor Parker, Head of Training and Curriculum at UKRA, told us that it was established to provide "accessible learning and development opportunities for those who have the responsibility to deliver resilience in the UK".[283] She said its primary audience is "resilience and emergencies practitioners" and highlighted its role in bringing organisations together to "plan, train and exercise together".[284] The 2026 Resilience Action Plan Implementation Report states that UKRA is expanding its training across the public and private sectors and civil society, and has developed "new career pathways to ensure high-quality, inclusive training and education".[285] UKRA held

275 Q 87 (Charles Collins)
276 Q 87 (Paul Griffiths)
277 HC Written Answer, 103960, Session 2024–26
278 French Ministry of the Armed Forces and Veterans Affairs, *National Service*
279 Written evidence from SafehousePro UK Ltd (NLR0030)
280 *Ibid.*
281 Written evidence from Armagh City, Banbridge and Craigavon Borough Council (NLR0122)
282 Written evidence from Simon Bradley (NLR0142)
283 Q 1 and QQ 5–6 (Dr Eleanor Parker)
284 *Ibid.*
285 Cabinet Office, *UK Government Resilience Action Plan: 2026 Implementation Report*, 14 July 2026

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

a Youth Engagement Day for 16–18-year-olds in June 2026, which it said demonstrated young people's interest in learning about resilience and contributing to their communities.[286] UKRA also reported that it had trained 2,869 people, alongside almost the same number attending other training, with a first-year target of 4,000 participants.[287]

188. However, follow-up information showed that 78% of UKRA participants were from the public sector, compared with 8% from the private sector and less than 1% from the voluntary sector.[288] This contrasts with the Government's stated ambition for UKRA to build skills "across the whole of society".[289] Finland's National Defence Courses draw participants from a wider range of sectors, including 32% from the commercial and industrial sectors, 19% from the media, labour and employer organisations and NGOs, and 17% from public administration, alongside participants from Parliament and political parties, universities and culture, and the Defence Forces.[290] During our visit to Finland, we heard that the courses are a central part of Finnish preparedness culture. Attendance is by invitation, with an annual selection process, and is intended to reach key decision-makers, including chief executives, directors and leaders of non-governmental organisations and faith groups. The courses are funded by the Finnish Ministry of Defence at around one million euros a year. We were told that selection is regarded as an honour, and that by the end of 2026 around 75% of members of the Finnish Parliament will have attended.[291]

189. Evidence highlighted the role of education and community engagement in countering disinformation and misinformation. The Cabinet Office said that community organisations have "a significant role to play" in strengthening resilience to false information,[292] and Byron Hyde argued that "Misinformation is best tackled by building critical thinking".[293]

190. We also heard that specialist technological capability is increasingly important to national resilience. The Alan Turing Institute told us that "Sovereign AI capability is a resilience requirement" and highlighted the need to maintain a domestic research and technology base with sufficient technical expertise.[294] It described AI as both a source of new vulnerabilities and a means of strengthening resilience, including through cyber defence, environmental forecasting and the protection of critical infrastructure.[295] It also warned against excessive dependence on overseas cloud services and other technologies that may not remain available during disruption.[296]

191. **Education and training are fundamental to building a more resilient society, yet practical preparedness and resilience skills are not sufficiently embedded across the population. These capabilities should be developed throughout life rather than treated as specialist knowledge for resilience professionals.**

---

286 Correspondence, *Chief Executive Officer of the UK Resilience Academy*, 14 September 2026
287 Correspondence, *Chief Executive Officer of the UK Resilience Academy*, 30 June 2026
288 *Ibid.*
289 Written evidence from Cabinet Office (NLR0126)
290 Colonel Jussi Kosonen, Director, National Defence Courses Presentation (unpublished)
291 See Appendix 7.
292 Written evidence from the Cabinet Office (NLR0126)
293 Written evidence from Byron Hyde (NLR0070)
294 Written evidence from the Alan Turing Institute (NLR0091)
295 *Ibid.*
296 *Ibid.*

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

192. **National resilience also increasingly depends on specialist technological capability. The UK's reliance on AI, cloud, cyber and other emerging technologies creates a need to build and retain domestic expertise while reducing critical dependencies on overseas providers.**

193. ***We recommend that the Government develop a life-long national programme for resilience education and skills. This should embed practical preparedness, critical thinking and information literacy from an early age and reinforce these skills through further and higher education, workplaces and community learning. It should include the skills needed to identify and respond to misinformation and disinformation.***

194. ***We recommend that the Government expand the reach of the UK Resilience Academy beyond the public sector, with substantially greater participation from businesses and civil society. UKRA should establish a national resilience course for senior leaders, modelled on Finland's national defence courses, bringing together chief executives, directors, senior officials, parliamentarians, media professionals and leaders from civil society and faith organisations to build relationships and shared preparedness before crises occur.***

195. ***We recommend that the Government develop a programme to strengthen specialist skills in AI, cloud, cyber and other emerging technologies critical to national resilience. This should build and retain domestic technical capability, reduce critical dependencies on overseas providers and ensure that emerging technological risks are identified and addressed.***

196. ***We recommend that the Government and the Armed Forces step up the plans to expand the Armed Forces 'Gap Year' Foundation Scheme with a vigorous public information campaign including targeting all those who are currently not in education, employment or training.***

Exercising and Stress Testing

197. High-level exercising is an important means of testing plans, interdependencies and decision-making before a crisis occurs. Polly Copeman told us that exercises should create "scenarios that we can fail and learn from within a safe environment", allowing participants to "stress-test the decision-making".[297] Margaret Read similarly emphasised the importance of "thinking across the whole system, rather than just on a sector-by-sector basis".[298]

198. Professor Nicola Ranger pointed to the financial sector as an example of a sector in which regular stress testing and scenario analysis are already well established. She told us that "all financial institutions in the UK, particularly banks, are required to conduct regular stress testing and scenario analysis against any material financial risks" and argued that this approach should be extended to other sectors where failure could have a significant impact on national resilience.[299]

297 Q 135 (Polly Copeman)
298 Q 135 (Margaret Read)
299 Q 135 and Q 138 (Professor Nicola Ranger)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

199. Exercise Pegasus was a UK-wide pandemic preparedness exercise held in autumn 2025. It tested the response to a novel pandemic across Government departments, the devolved administrations and Local Resilience Forums, with participation from businesses and voluntary and community organisations.[300] Mark Samuels, who took part in the exercise, described it as "incredibly important", but cautioned that there was an element of "fighting the last war" because of its focus on a pandemic scenario.[301] The Government has published initial lessons, with the full post-exercise report expected in winter 2026.[302]

200. A further tabletop exercise, Exercise Tucana, was held in July 2026 to examine health-system preparedness in a major national security crisis. Public reporting indicated that around 120 participants from the NHS, Ministry of Defence, Cabinet Office and wider civil society took part in an escalating scenario involving disruption to critical infrastructure and large numbers of military and civilian casualties.[303] The exercise was reported to have identified pressures on casualty management, workforce mobilisation and healthcare surge capacity, although the Government had not formally evaluated the exercise at the time of publication.[304]

201. The Government has announced that Exercise Albiston Shadow will take place in 2027 and will be the largest UK home defence exercise in decades.[305] The multi-day exercise will test Government preparedness for hybrid attacks against the UK and is expected to involve ministers and hundreds of officials from across Government and the public sector.[306] It will complement NATO's CMX27 crisis-management exercise.[307]

202. We also heard that UK national defence plans will be tested through NATO's Steadfast Defender 27. Damian Johnson described this as the "largest mobilisation exercise since the Cold War".[308] Lt-Gen Griffiths told us that Steadfast Defender would be run alongside the domestic Brave Defender series, allowing the UK to test "the Article 3 homeland bit and the Article 5 bit, and how the tensions between the two are played through".[309] Separately, the 2025 UK Government Resilience Action Plan committed to a new National Exercising Programme, with annual national exercises across a range of risks and involving actors from across society to test the UK's resilience in practice.[310]

203. **We welcome the increase in national exercising, including plans to test a wider range of threats and involve organisations across society. Exercises are most valuable when they expose weaknesses before a real emergency. We agree with the evidence that exercising should provide a safe environment in which organisations can "fail and learn". National exercises should therefore be sufficiently demanding**

300 Cabinet Office, *UK Government Resilience Action Plan: 2026 Implementation Report*, 14 July 2026
301 Q 154 (Mark Samuels)
302 Cabinet Office, *UK Government Resilience Action Plan: 2026 Implementation Report*, 14 July 2026
303 The Times, *Stockpile food, water and medicine to prepare for war, Britons to be told*, 15 July 2026
304 *Ibid.*
305 Cabinet Office, *Risk of democratic interference added to National Risk Register*, 14 July 2026
306 *Ibid.*
307 *Ibid.*
308 Q 78 (Damian Johnson)
309 Q 86 (Paul Griffiths)
310 Cabinet Office, *UK Government Resilience Action Plan*, 8 July 2025, para 71

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

to identify where plans, systems and cross-sector dependencies break down.

204. **It is not clear who is responsible for setting standards for resilience stress testing, assessing performance and ensuring that lessons identified through exercises are implemented.**

205. ***We recommend that the Government apply the stress-testing approach used in the financial sector to national resilience. It should establish regular cross-sector stress tests for critical sectors, including food, energy and water, pharmaceuticals and other strategically important industries, involving central and local Government, the Armed Forces, Local Resilience Forums, the voluntary and community sector, and relevant businesses. It should also set out who will oversee this regime, including whether an existing regulator or a dedicated body should be responsible for setting standards, monitoring compliance and ensuring that lessons are acted upon.***

Volunteers and Civil Reservists

206. We heard that volunteering is an effective way of engaging large numbers of people in supporting national resilience. The British Red Cross highlighted the importance of "mobilising volunteer capacity" and told us that the voluntary and community sector brings "insight, expertise and capacity" which should be genuinely engaged in resilience planning and delivery.[311] It also cautioned that "Voluntary activity is part of the solution but is not 'free'", requiring sustained capacity and resources.[312] Neil Cameron similarly warned against over-reliance on volunteers, noting that volunteers and third-sector staff may themselves have vulnerabilities which "may prohibit their action and support depending on the emergency".[313]

207. Volunteer capacity is most effective when it is organised and embedded within existing local structures. Marcus Lions argued that established organisations such as parish councils, Scout groups, faith organisations, sports clubs and community centres already provide the trust, premises and communication channels needed to mobilise people effectively.[314] The VCS Emergencies Partnership (VCSEP) similarly highlighted mechanisms such as the Cumbria Volunteering Portal, which allows people to register in advance for emergency-response roles.[315]

208. Despite this potential, the voluntary sector is not sufficiently embedded within existing resilience structures. The VCS Emergency Partnership highlighted difficulties coordinating spontaneous volunteers during emergencies, warning that inadequate arrangements for training, safeguarding and health and safety could create avoidable risks for volunteers, responders and communities.[316] Witnesses argued for earlier and more formal integration of the voluntary sector into preparedness and response.[317]

---

311 Written evidence from British Red Cross (NLR0056)
312 *Ibid.*
313 Written evidence from Neil Cameron (NLR0020)
314 Written evidence from Marcus Lions (NLR0075)
315 Written evidence from the VCS Emergencies Partnership (NLR0151)
316 Written evidence from the VCS Emergencies Partnership (NLR0061)
317 Q 169 (Matt Killick); written evidence from the VCS Emergencies Partnership (NLR0061)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

209. Witnesses identified veterans and other experienced professionals as an underused source of specialist resilience capability, particularly in leadership, logistics and emergency planning.[318] One witness proposed a National Resilience Expert Register to enable relevant expertise to be identified and mobilised rapidly during emergencies.[319]

210. Witnesses raised concerns that military mobilisation could create competing demands for people who also perform important civilian or voluntary resilience roles. The Ministry of Defence acknowledged that reservists may be required in their civilian employment during a crisis and "would not necessarily" be mobilised into a different role.[320] The FCDO also maintains civilian surge capacity through its Civilian Stabilisation Group, a roster of more than 450 deployable experts across 17 conflict capabilities, alongside a separate roster of deployable humanitarian experts for rapid-onset and protracted emergencies.[321] The Civilian Stabilisation Group made more than 190 deployments in the previous 12 months.[322]

211. Emergency services are beginning to assess this risk. Alex Woodman told us that the fire and rescue sector was working with military colleagues on "mapping and modelling" reservist commitments and said that this work "needs to accelerate".[323] The police estimated that around 2.2% to 2.9% of officers in most forces undertake voluntary reserve roles, although further work is under way to assess strategic reserve commitments.[324] Matt Killick warned that St John Ambulance faced a "significant risk" of losing volunteers who are also military reservists or healthcare professionals during concurrent demands.[325]

212. We heard that the MoD has developed Plan Fortitude to support the UK's NATO resilience obligations. Lt-Gen Griffiths described four elements: Reliance, which connects Defence with wider society; Sentinel, concerned with protecting Defence infrastructure; Genesis, focused on mass mobilisation; and Forge, which supports the movement of UK and allied forces. He said that Genesis would consider increasing the military workforce, "perhaps with civilian volunteers to support us in times of crisis and conflict".[326]

213. The International Committee of the Red Cross cautioned that greater civilian involvement in national defence also raises legal and protection concerns. It warned that involving civilians in military operations or using civilian infrastructure for military purposes can "blur the line between combatants and civilians" and increase the risk that civilians or civilian infrastructure are perceived as contributing to hostilities. It concluded that "the more civilian infrastructure is used—or designated for use—for military purposes, the greater the danger for harm".[327]

---

318 Written evidence from the Defence Gardens Scheme Community Interest Company (NLR0158)
319 Written evidence from Mark Brown (NLR0105)
320 Q 84 (Damian Johnson)
321 Correspondence, *Foreign, Commonwealth and Development Office*, 25 September 2026
322 *Ibid.*
323 Q 162 (Alex Woodman)
324 *Ibid.*
325 Q 162 (Matt Killick)
326 Q 78 (Paul Griffiths)
327 Written evidence from the International Committee of the Red Cross (NLR0146)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Box 3: Civil protection initiatives

The UK has previously maintained a number of organisations intended to provide additional civil protection and emergency capacity. The Civil Defence Corps, established in 1949, was a civilian volunteer organisation intended to support local authorities following a major national emergency.[328] It reached approximately 330,000 members in the 1950s before being stood down in 1968. The Royal Observer Corps, composed largely of part-time volunteers, had a civil-defence role during the Cold War and was stood down in 1995.[329] The Home Service Force, established in 1982 as a volunteer military home-defence force, was disbanded in 1992.[330]

More recent Governments have sought to encourage civic participation through different models. The Big Society programme, launched in 2010, aimed to strengthen community participation, voluntary activity and local decision-making.[331] It included the creation of the National Citizen Service, which subsequently operated as a national youth programme until 2025.[332] The Government's 2018 Civil Society Strategy also sought to strengthen the role of communities, charities and social enterprises.[333]

Proposals for more formal reserve capacity have also been considered. The 2020 Kruger review proposed a "volunteer passport" and a National Volunteer Reserve to make it easier to mobilise citizens for public service.[334] The Government did not adopt the proposed passport.[335] Separately, the 2021 Integrated Review committed the Government to consider "a civilian reservist cadre for support in times of crisis"[336]; this commitment did not appear in the 2023 Integrated Review Refresh.[337]

Outside Government, proposals have also been developed for a UK Civil Reserve, comprising trained volunteers who could be mobilised during major incidents or national emergencies,[338] and a National Resilience Corps, which would train and organise civilian volunteers to support essential services and communities during crises.[339]

214. **Military reservists, veterans and other skilled volunteers could provide valuable additional capacity during national emergencies. However, we are concerned that the same individuals may be relied upon simultaneously by the Armed Forces, emergency services, healthcare and voluntary organisations. Without a clear understanding of these competing demands, resilience plans risk overstating the personnel available during a major or concurrent crisis.**

328 HC Deb, 15 December 1965, col 303
329 HC Deb, 16 December 1991, col 16
330 HC Deb, 3 March 1982, cols273–282
331 HM Government, *Cameron and Clegg launch The Big Society* (May 2010)
332 *Ibid.*
333 HM Government, *Civil Society Strategy: building a future that works for everyone* (9 August 2018)
334 Danny Kruger MP, *Levelling Up Our Communities: Proposals for a New Social Covenant*, September 2020
335 Cabinet Office, *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*, 16 March 2021
336 *Ibid.*
337 Cabinet Office, *Integrated Review Refresh 2023: Responding to a more contested and volatile world* (CP 811, 13 March 2023)
338 United Kingdom Civil Reserve, *About Us*
339 Think Labour, *A New Civil Partnership*, September 2026

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

215. ***We recommend that a national register of volunteers and civil reservists, focused on specialist skills and knowledge, should be developed and maintained. This should be developed through a national campaign and modelled on the NHS Volunteer Responders programme developed in COVID-19. The data exist but need to be reconfigured to identify existing volunteers, recruit new ones and ensure that they are given things to do in a crisis.***

216. ***We recommend that the Government explore the introduction of an entitlement to paid civic resilience leave, enabling employees to undertake approved training, exercising and emergency volunteering without loss of income. It should work with employers to establish proportionate arrangements and encourage wider participation across the workforce.***

217. ***We recommend that the Government require local authorities, working with Local Resilience Forums and voluntary and community organisations, to establish and maintain registers of local volunteers. These should identify relevant skills and capabilities and enable volunteers to be mobilised quickly and effectively during emergencies.***

Funding

218. In response to the worsening threat environment, the UK and its NATO allies agreed to increase investment in defence and security to 5% of GDP by 2035. This comprises at least 3.5% of GDP for "core defence requirements" and up to 1.5% for broader defence- and security-related investments, including protecting critical infrastructure, defending networks, ensuring civil preparedness and resilience, innovation and strengthening the defence industrial base.[340] The Government has not yet set out a detailed breakdown of how spending under the 1.5% resilience and security component will be allocated or what additional resilience capabilities it will deliver.[341]

219. Despite these funding commitments, concerns remain about whether local capability is adequately resourced. SafehousePro argued that the gap between national ambition and local capability remains one of "infrastructure, resourcing and accountability".[342] By comparison, Sweden has pursued sustained increases in civil-preparedness funding. Its Ambassador told us that funding had risen from around £200 million in 2022 to £1 billion in 2026, a "five-fold increase in four years".[343] The Swedish Government plans further increases through to 2028 as part of what it describes as the most substantial reinforcement of its total defence since the Cold War.[344]

220. The Government agreed a £22 million three-year funding settlement for Local Resilience Forums (LRFs) from 2022/23, alongside a further £3.5 million for the 2026/27 Stronger LRF Trailblazer Programme.[345] It also established a £2.5 million Civil Society Resilience Infrastructure

340 NATO, *Defence investment and NATO's 5% commitment*, 29 June 2026
341 Joint Committee on the National Security Strategy, *The National Security Strategy* (4th Report, Session 2024–26, HC Paper 1045, HL Paper 281)
342 Written evidence from SafehousePro UK Ltd (NLR0030)
343 Q 23 (Stefan Gullgren)
344 Government Offices of Sweden, *New package for stronger civil defence*, 17 September 2025
345 HC Written Answer, 170752, Session 2022–23; Cabinet Office, *The UK Government Resilience Action Plan: 2026 Implementation Report*, July 2026.

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Fund for 2026–29.[346] Despite these initiatives, concerns remain about the adequacy and sustainability of funding, with Bedfordshire LRF describing it as "inadequate and unstable"[347] and the Government acknowledging that local resilience funding can be "fragmented, short-term, and fall short of requirements".[348]

221. **The move towards multi-year funding for Local Resilience Forums is welcome, but local resilience has too often depended on short-term and fragmented funding. Effective local resilience depends on sustained and predictable investment that enables local structures to retain skilled staff, build enduring partnerships and develop capability.**

222. ***We recommend that the Government set out a clear plan for how part of the 1.5% of GDP specified for 2035 will be spent on civil preparedness and resilience. It should break down planned spending and explain how resources will be allocated.***

Home defence

223. Several witnesses argued that the civil and military components of national defence need to be more closely aligned. The Norwegian Ambassador, HE Tore Hattrem, told us that his Government's policy was to strengthen the military and civil preparedness together, and that this integrated approach was one he did not see in the same way in the UK.[349]

224. Paddy McGuinness told us that current arrangements assume support flows in one direction. Under military aid to the civil authorities, the Armed Forces assist civilian responders when civil capacity is exceeded, as during the flooding of the Somerset Levels or the foot and mouth outbreak.[350] He argued that in a conflict this relationship would be inverted, and that "the civilian authorities will have to support the military", as they did in the Second World War when national activity was directed towards enabling war fighting.[351]

225. Witnesses acknowledged that the UK cannot fully replicate models used elsewhere. Baroness Neville-Jones said that, while the UK would not go as far as Finland, "there is a lot that we can learn".[352] Box 2 sets out how several partner countries integrate civil and military preparedness, and Box 3 describes the civil protection organisations the UK has previously maintained.

226. The Government's approach has developed to some extent during this Parliament. Damian Johnson told us that the Home Defence Programme should include "a whole-of-society approach, working across national, devolved and local government, first responders, industry, academia, civil society and the public".[353] Roger Hargreaves said that the programme involved "rebuilding the war books", operational plans for conflict, major

346 Cabinet Office, *The UK Government Resilience Action Plan: 2026 Implementation Report*, July 2026.
347 Written evidence from Bedfordshire Local Resilience Forum (NLR0130)
348 Cabinet Office, *UK Government Resilience Action Plan*, 8 July 2025
349 Q 18 (Tore Hattrem)
350 Q 190 (Paddy McGuinness)
351 *Ibid.*
352 Q 190 (Baroness Neville-Jones)
353 Q 78 (Damian Johnson)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

exercises and the acquisition of new capabilities.[354] However, Lt-Gen Collins confirmed that a total defence model was not something the Government was pursuing at present, although there was scope for a broader form of voluntary reserve service.[355] Dame Angela Eagle MP supported this and told us that "every approach fits the geography and situation that the country is in."[356] She said that whole-society training was "probably a bit extreme" for the UK's approach, but that the Government sought to draw best practice from NATO allies.[357]

227. **The Government is right to rebuild its home defence arrangements, but the relationship between civilian resilience and military defence remains underdeveloped. In a major conflict, civilian institutions are likely to have to support military operations while maintaining essential services, yet the responsibilities and arrangements involved are not sufficiently defined or tested.**

228. **While the UK does not need to replicate other countries' total defence models, there is much to learn from their approaches to integrating civilian and military preparedness, particularly given the shared threats we face.**

229. ***We recommend that the Government use the Home Defence Programme to define how civilian and military preparedness will work together in practice. It should clarify the roles of government, local responders, critical infrastructure operators and other civilian partners in supporting defence and test these arrangements through regular training and cross-government exercises.***

354 Q 203 (Roger Hargreaves)
355 Q 87 (Charles Collins)
356 Q 210 (Angela Eagle MP)
357 *Ibid.*

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

CHAPTER 5: COMMUNICATIONS AND DEVELOPING A CULTURE OF RESILIENCE

230. Has preparedness become part of everyday life in the UK, or is it still something we think about only when a crisis occurs? This chapter considers what is needed to develop a culture in which individuals, communities, businesses and Government understand the risks they face and routinely take action to prevent or prepare for them.

231. Turning resilience from a theoretical concept into practical readiness depends on how, when and through which channels key messages are communicated. Trust, confidence, transparency and the normalisation of preparedness do not arise from publishing advice alone. People need messages they understand, delivered by credible sources, which are linked to clear actions they can take.

Information environment

232. The National Preparedness Commission said that "public trust in government and its institutions is declining"[358] while Sam Wise, Chief Strategy Officer at Saatchi and Saatchi, said that trust in " … everything which is closer to [people] is increasing."[359] Lloyd's Register Foundation pointed to findings from its World Risk Poll, conducted in 2019, 2021, 2023 and 2025, which consistently found that 40% of people consistently said Government did not care about their wellbeing.[360]

233. There was evidence, however, that some organisations retain substantial public trust. Nancy Hey said that in a global context, "the UK has much higher than average trust in local news and weather for information about disasters".[361] Alex Woodman and Mark Williams said that their branches of the emergency services were trusted by the public.[362]

234. There was mixed evidence on the extent to which the BBC is trusted. Rhodri Talfan Davies, Deputy Director General at the BBC, told us that trusted news, such as that coming from the BBC, becomes particularly important during national crises.[363] However, we heard that trust in centralised sources, including national broadcasters, was declining, with research showing that the proportion of people likely to turn first to national television during a serious event had fallen from 82.6% to 50.8%.[364]

235. Pupils 2 Parliament found that the secondary school students it consulted were most likely to turn to their parents for trusted information during an emergency, followed by Government sources, news outlets, including the BBC, and the emergency services. However, pupils also expressed concerns about the reliability of information, with 29 of the 43 consulted saying they would not trust social media and 16 expressing distrust of AI-generated information.[365]

358 Written evidence from the National Preparedness Commission (NLR0004)
359 Q 93 (Sam Wise)
360 Written evidence from Lloyd's Register Foundation (NLR0057)
361 Q 93 (Nancy Hey)
362 Q 145 (Alex Woodman, Mark Williams)
363 Q 140 (Rhodri Talfan Davies)
364 Q 93 (Sam Wise)
365 Written evidence from Pupils 2 Parliament (NLR0165)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

236. Witnesses told us that public awareness of national-scale risks is limited and largely confined to what people can see locally. The Resilience Imperative wrote that there is limited awareness of risks such as cyber-attacks, extreme weather, societal instability and biological hazards.[366] Lord Harris said that "the bulk of the population is blissfully unaware of some of the risks" and the pace at which they are changing.[367]

237. Despite limited awareness of specific national risks, there was evidence of growing public concern about the possibility of major crises. Nancy Hey related data from her organisation's World Risk Poll which showed that two-thirds of people were concerned about risks and that war had newly appeared as a concern.[368] Sam Wise told us that the proportion of people rating a serious UK crisis within ten years as certain or very likely had risen from 30% to 70% since 2019.[369] Dr Parker explained that "the public have a good understanding of the risks that they face" but not "the actions that they can take to prepare".[370]

238. Witnesses emphasised the importance of greater openness with the public about the risks facing the UK. Mfon Akpan of the NAO said that Government should "treat society and the public as mature adults" and not be "scared about the underlying risk".[371] Paddy McGuinness warned against a reluctance to "spook the public", arguing that withholding information about known risks, or failing to communicate it clearly, could ultimately alienate the public.[372] We heard that Sweden provides honest information to the public about risks and "manages to do this without scaring people".[373]

Disinformation and misinformation

239. We were told about issues connected with disinformation and misinformation. Sam Wise said that "there has to be a distinction between disinformation, which is malicious, and what can loosely be called misinformation, where people are putting out things which are not necessarily true".[374] M&C Saatchi World Services wrote that disinformation "typically attaches to real events, amplifying emotionally charged narratives that spread rapidly".[375]

240. Evidence described practical effects of disinformation and misinformation. Stephanie Buller wrote that "disinformation exploits gaps between national messaging and lived experience, reinforcing perceptions that preparedness advice is for 'other people'".[376] Alex Towers, Director of Policy and Public Affairs at BT Group, described pandemic-era misinformation resulting in physical attacks on critical communications infrastructure.[377] The Resilience Imperative related a Russian strategy to incite tension in the US using online information spread by bots.[378]

---

366 Written evidence from the Resilience Imperative (NLR0090)
367 Q 35 (Lord Harris of Haringey)
368 Q 92 (Nancy Hey)
369 Q 92 (Sam Wise)
370 Q 6 (Dr Eleanor Parker)
371 Q 6 (Mfon Akpan)
372 Q 198 (Paddy McGuinness)
373 Written evidence from Neil Cameron (NLR0020)
374 Q 101 (Sam Wise)
375 Written evidence from M&C Saatchi World Services (NLR0088)
376 Written evidence from Stephanie Buller (NLR0077)
377 Q 116 (Alex Towers)
378 Written evidence from The Resilience Imperative (NLR0090)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

241. Witnesses highlighted the growing challenge of countering disinformation and misinformation. Emerging Risks Global warned that AI could generate disinformation faster than it could be fact-checked.[379] Deborah Haynes, Security and Defence Editor at Sky News, described a recent Russian operation intended to discredit a counter-disinformation campaign run by the Government.[380]

242. Evidence stressed that countering disinformation depends on credible messengers and the ability to rebut quickly. The Emergency Planning Society wrote that "communications plans should include active monitoring, rapid rebuttal pathways, and the use of credible local intermediaries".[381] Rhodri Talfan Davies said that the BBC's "ability to challenge inaccurate information and verify video and audio sources is incredibly important".[382]

243. We heard how other countries have organised themselves to counter disinformation and misinformation. HE Stefan Gullgren, Ambassador of Sweden, told us about Sweden's Psychological Defence Agency "for detecting and resisting malign information influence directed at Sweden by antagonistic foreign powers".[383] RAND Europe said that in Ukraine, "advance warnings about likely false narratives reduced the credibility and impact of subsequent disinformation".[384]

244. The Government sought to provide reassurance that it was alive to the information environment. Roger Hargreaves said that the Government did learn from Scandinavian countries on public information.[385] However Dame Angela Eagle MP, said that "trust in institutions is low and people are not likely to listen" and that "the less trust and the more fragmented our society, the harder it is to get resilience".[386] She added: "If you are in a democracy and there is no agreement about what the truth is … you are in a very difficult situation".[387]

245. **Despite recent promising developments contained within the Be Ready campaign, the Government has failed to communicate national risks openly and consistently enough. Reluctance to discuss serious threats leaves people less prepared, undermines public trust and creates opportunities for misinformation and disinformation to spread. Poorly judged or inconsistent communication also risks provoking public backlash on social media, particularly where trust in Government is already low.**

246. ***We recommend that the Government adopt a more open approach to communicating national risks. It should provide regular, accessible and candid information about significant risks, their potential consequences and the actions being taken to mitigate them.***

247. ***We welcome the Prime Minister's announcement of the new National Centre for Information Defence. However, we recommend that the***

379 Written evidence from Emerging Risks Global (NLR0002)
380 Q 68 (Deborah Haynes)
381 Written evidence from the Emergency Planning Society (NLR0118)
382 Q 116 (Rhodri Talfan Davies)
383 Q 21 (Stefan Gullgren)
384 Written evidence from RAND Europe (NLR0139)
385 Q 211 (Roger Hargreaves)
386 Q 208 (Angela Eagle MP)
387 Q 211 (Angela Eagle MP)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Government must clarify its remit, responsibilities and how it will operate in practice. The Centre should be operationally independent and take a proactive approach to identifying, attributing and countering hostile information activity, working closely with international partners.

248. ***We recommend that the Government engage with a wide range of news outlets, including those which are not necessarily their natural partners, but which segments of the public trust, so key messages are heard by and reinforced to as many people as possible.***

Digital communications

249. Witnesses described how far the economy, essential services and emergency response now depend on digital communications. Sophie Greaves told us that "the resilience question is a whole-economy issue, because so much of what we do now runs on … internet infrastructure".[388] We heard that "communications, navigation, financial systems, emergency response, and military command all depend on continuous satellite availability".[389]

250. Evidence highlighted risks to subsea cables, which was the subject of a 2025 report by the Joint Committee on the National Security Strategy (JCNSS).[390] Anthony Heron wrote that "subsea cables form the backbone of global connectivity, carrying roughly 95% of data traffic".[391] Alex Towers told us that BT had access to only two repair ships: one French-owned and generally unavailable, and one UK-based but 35 years old.[392] Sophie Greaves suggested that a significant proportion of breakages to cables are not accidental and called for Government-industry partnership on cable resilience because the telecommunications sector cannot fund the necessary measures alone.[393]

251. The UK's dependence on space-based infrastructure also raises questions about sovereign capability and resilience. This was previously discussed in the House of Lords 2025 UK Engagement with Space Committee.[394] Viasat UK said that satellites underpin communications and critical infrastructure and that the UK must protect its "sovereign interests in space".[395] UK Defence First called for a sovereign space strategy involving investment in domestic launch sites, revival of satellite manufacturing, and accelerated development of resilient systems.[396]

252. Resilience also depends on whether communications networks can continue operating during major disruption. Nihal Newman said that Ofcom requires operators to avoid single points of failure, build redundancy, and maintain business continuity procedures, but that often these "are not understood" and "are not tested".[397] Alex Towers said that BT's networks are resilient

388 Q 116 (Sophie Greaves)
389 Written evidence from ECAPS AB (NLR0089)
390 Joint Committee on the National Security Strategy, *Subsea telecommunications cables: resilience and crisis preparedness* (1st Special Report, Session 2024–26, HC Paper 1574, HL Paper 237)
391 Written evidence from Anthony Heron (NLR0027)
392 Q 124 (Alex Towers)
393 Q 124 (Sophie Greaves)
394 UK Engagement with Space Committee, *The Space Economy: Act Now or Lose Out* (Report of Session 2024–26, HL Paper 190)
395 Written evidence from Viasat UK (NLR0132)
396 Written evidence from UK Defence First (NLR0019)
397 Q 107 (Nihal Newman)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

to specific local and regional incidents, but that BT could not claim that a widespread national outage was fully covered.[398]

253. The Royal Academy of Engineering highlighted the importance of analogue radio as an alternative means of communication during emergencies, citing its vital role during Storm Desmond in 2015 when power and mobile networks failed in Lancaster.[399]

254. Emergency Alerts are one of the Government's main tools for communicating quickly with the public during life-threatening situations, with messages issued to mobile phones in English and Welsh only.[400] Vival Corporation wrote that "the UK's Emergency Alert system is a valuable tool for broadcast notification, but it represents only one moment in a longer preparedness chain".[401] Audiebant Ltd warned that the effectiveness of Emergency Alerts depends on maintaining public trust in the system, particularly when it is needed during a serious emergency.[402]

255. In August 2026, the Government issued an Emergency Alert addressing the risk of wildfires. It said that this reflected "the seriousness with which the government is acting to safeguard people and property".[403] The National Fire Chiefs Council said that there had been a decrease in the number of wildfires emergency services had responded to following the alert.[404] The lack of advance warning for the alert was criticised by charities and domestic abuse survivors, who said there was little chance to protect those hiding secret phones.[405] Questions were also raised over whether the alert met the threshold for use of the system, with the system's former designers also calling for greater clarity over the criteria governing its deployment.[406]

256. Witnesses also raised concerns about maintaining universal access to Digital Terrestrial Television (DTT). Broadcast2040+ warned that the Government's intention to reduce or end DTT from the mid-2030s would require households to receive television through broadband. It added that this would "weaken national resilience by reducing universal access", including among vulnerable people.[407] Rhodri Talfan Davies said that broadcasters and the Government must ensure that people who depend on DTT are supported through the transition to digital services.[408]

257. The Government set out the measures currently in place to maintain communications with the public during emergencies and outages. The Cabinet Office said that its Emergency Alerts system is capable of distributing life-saving information quickly and is maintained through regular testing.[409] Roger Hargreaves told us that the Government has "the arrangements with

398 Q 120 (Alex Towers)
399 Written evidence from the Royal Academy of Engineering (NLR0131)
400 HM Government, *About Emergency Alerts*
401 Written evidence from Vival Corporation Ltd (NLR0009)
402 Written evidence from Audiebant Ltd (NLR0045)
403 Cabinet Office, *Emergency Alert to be sent to England and Wales as Government steps up wildfire response with funding, military support and BBQ ban*, 14 August 2026
404 National Fire Chiefs Council, *Wildfire Update: Continued Vigilance Needed*, 17 August 2026
405 BBC News, *Wildfire Phone alert was 'entirely appropriate', government says*, 17 August 2026
406 BBC News, *We helped create UK emergency alert system — but question how government is using it* , 29 August 2026
407 Written evidence from Broadcast2040+ (NLR0042)
408 Q 116 (Rhodri Talfan Davies)
409 Written evidence from the Cabinet Office (NLR0126)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

broadcasters to put out emergency broadcasts when power is absent".[410] The Minister said that the Government would encourage households to keep batteries and wind-up radios or battery-powered radios.[411]

258. **National resilience is heavily reliant on digital communication, but the supporting infrastructure remains vulnerable to power outages and/or damage to subsea cables. Existing mitigations are not yet sufficiently rigorous or enduring to guarantee communications through prolonged disruption. Older technologies also remain important where digital communications fail, making the Government's dependence on digital systems without comprehensive back-up arrangements a significant resilience weakness.**

259. ***We recommend that the Government develop, with the telecommunications and digital infrastructure sectors, a response plan in the event of widespread national power outages, subsea cable disruption, and any other means of interference, which sets out plans for the deployment of resilient back-up communications across different scenarios, and mandates regular testing of business continuity arrangements. The Government should also bring forward legislation to implement the proposals in its October 2026 White Paper on Critical Undersea Infrastructure Security and Resilience.***

260. ***We recommend that the Government should abandon its plan to switch off Digital Terrestrial Television, which risks weakening national resilience by reducing universal access to communication, as well as learn lessons from the switching off of the Public Switched Telephone Network on 31 January 2027.***

Individual mindset and public communication

261. Evidence identified several traits associated with individual resilience. Emerging Risks Global defined psychological resilience as "the capacity of individuals to manage stress, maintain function and recover from adverse experiences".[412] Ian Fox emphasised the importance of developing practical competence so that "calm judgement, reasonable response, and mutual support" become normal behaviours.[413] Alfred Malmros said that younger generations sometimes want to be "in control, in charge of themselves, having agency and being prepared for whatever hits them".[414]

262. Witnesses pointed to previous campaigns that had successfully changed public behaviour. Stephen Arundell described counter-terrorism campaigns that used celebrities, slogans, online activity and information packs in schools and universities.[415] Grand Challenge AI cited the rail network's slogan "See it, Say it, Sorted" as a behavioural campaign model.[416] M&C Saatchi World Services said that, during the pandemic, the authority of the Chief Medical

410 Q 208 (Roger Hargreaves)
411 Q 208 (Angela Eagle MP)
412 Written evidence from Emerging Risks Global (NLR0002)
413 Written evidence from Ian Fox (NLR0001)
414 Q 97 (Alfred Malmros)
415 Q 49 (Stephen Arundell)
416 Written evidence from Grand Challenge AI (NLR0105)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Officer and Chief Scientific Adviser was "instrumental in ensuring that demanding restrictions were understood and followed".[417]

263. Evidence supported adapting national messages for different audiences. The Resilience Imperative said that "risk communication should be co-designed and distributed through [local] networks rather than being broadcast from the top down".[418] The National Emergencies Trust said that joint communications involving the Government, local Government, Local Resilience Forums and civil society were essential.[419]

264. Evidence suggested that effective communication with young people depends on trusted messengers, appropriate language and the platforms they use. Becky Heginbotham-Blount wrote that young people "prefer to be communicated with [by] people their own age, using their own language on platforms they use".[420] Alfred Malmros said that smaller online influencers could be more relevant to some young people than personalities with very large audiences.[421]

265. Evidence also considered communication with vulnerable people. Business in the Community wrote that "for vulnerable groups, communication should be practical, accessible, and tailored to the barriers people face".[422] Lloyd's Register Foundation called for "targeted outreach to lower-income groups and high-risk regions".[423]

266. Some witnesses expressed caution about messaging which urges people to make preparations which might not be appropriate for certain groups. Simon Bradley noted that "highly vulnerable demographics cannot afford to stockpile".[424] Dr Otley of VCSEP warned that inequality must not be compounded by communicating only with people who already have the ability to prepare.[425]

267. Witnesses stressed the importance of providing accessible, multilingual communications during emergencies. The Chartered Institute of Linguists, the All-Party Parliamentary Group on Modern Languages and the National Register of Public Service Interpreters highlighted the need for professional language support to ensure accurate and effective communication.[426] The All-Party Parliamentary Group on Modern Languages said that the Grenfell Tower disaster exposed the absence of multilingual communications capability.[427] ISC2 pointed to Norway's emergency preparedness leaflet, which has been translated into 30 languages.[428]

---

417 Written evidence from M&C Saatchi World Services (NLR0088)
418 Written evidence from The Resilience Imperative (NLR0090)
419 Written evidence from the National Emergencies Trust (NLR0114)
420 Written evidence from Becky Heginbotham-Blount (NLR0014)
421 Q 93 (Alfred Malmros)
422 Written evidence from Business in the Community (NLR0166)
423 Written evidence from Lloyd's Register Foundation (NLR0057)
424 Written evidence from Simon Bradley (NLR0142)
425 Q 77 (Dr Carolyn Otley)
426 Written evidence from the Chartered Institute of Linguists (NLR0028); the All-Party Parliamentary Group on Modern Languages (NLR0112); the National Register of Public Service Interpreters (NLR0100)
427 Written evidence from the All-Party Parliamentary Group on Modern Languages (NLR0112)
428 Written evidence from ISC2 (NLR0050)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Guidance

268. Witnesses emphasised that preparedness advice must enable people to take practical action.[429] Nancy Hey said that "knowing that there are things you can do and a pathway to get there are the ingredients for hope".[430] The Be Ready campaign (and Prepare website before it) begins that journey.

269. We heard about a range of practical measures households could take to improve their preparedness. Witnesses recommended practical household preparations, including supplies of food and water, alternative heating and cooking arrangements, emergency kits and evacuation plans.[431] LINK also recommended keeping sufficient cash for three to four days in case ATMs were unavailable during power outages, suggesting £50 per adult and £25 per child.[432]

270. Several witnesses questioned whether a 72-hour preparedness baseline was sufficient or achievable for all households. Neil Cameron warned that "Cost may be a factor for some and prohibit their preparedness and resilience", and noted that power disruption during Storm Arwen lasted "for some up to 10 days".[433] Evidence from researchers at the University of Strathclyde also noted that, following a GB-wide power system collapse, the new restoration standard allows up to five days for full demand to be restored.[434] Professor Lang described the Prepare website as "too limited", arguing that advice centred on "a few bottles of water and a few days of food" did not adequately address wider risks to food security.[435]

271. In Finland, the 72-hour figure is not intended to cover the whole of a disruption. Households are asked to hold three days of supplies on the basis that they would then be able to buy a further three days of food in stores. The guidance is to keep a rolling buffer of three days of the things a household normally uses, so that nothing goes out of date.[436] A yearly survey found that around half of Finns hold three days of stock in line with the guidance.

272. The National Preparedness Commission warned that the Prepare website, which is now called Be Ready, could be difficult to access "during a power or internet outage" and called for preparedness information to be reinforced through household booklets, broadcast and social media, and public places such as libraries.[437] The National Association of Local Councils highlighted Emergency Liaison Points in St Ives which can "operate without power, telephones or internet", providing trusted information and support during disruption.[438]

273. Witnesses told us about resilience booklets used in other countries. HE Ambassador Kristina Beckvard of Denmark said that Danish guidance advised citizens to keep water, food, medicine, hygiene supplies, communications

429 Q 105 (Prof Lee Miles); Q 98 (Alfred Malmros)
430 Q 98 (Nancy Hey)
431 Written evidence from Coastal Survival School (NLR0168); written evidence from Dr Dolapo Fakuade and Dr Justin Okoli (NLR0127)
432 Written evidence from LINK ATM (NLR0036)
433 Written evidence from Neil Cameron (NLR0020)
434 Written evidence from Jane Wright, Dr James Irvine and Dr Keith Bell (NLR0107)
435 Q 118 (Prof Tim Lang)
436 See Appendix 7.
437 Written evidence from the National Preparedness Commission (NLR0004)
438 Written evidence from the National Association of Local Councils (NLR0041)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

equipment and cash.[439] HE Stefan Gullgren linked Sweden's household booklet to "public support through awareness of risk, readiness to act and trust in institutions".[440] Vival Corporation said of Sweden's booklet: "It tells citizens precisely what to do, and it is culturally normalised".[441]

274. Dame Angela Eagle MP told us that the Government did not intend to distribute preparedness booklets to every household, instead relying on its website.[442] She said that households were advised to maintain a 72-hour supply of essentials, including food, water, batteries and medicines, and that the Government's planned public preparedness campaign would provide practical advice without alarming the public, building awareness over time.[443]

275. **A Government website is inadequate as the principal means of communicating resilience advice. Reliance on digital guidance risks excluding some groups, particularly during power or internet outages. The advice is also insufficient for prolonged or severe disruption.**

276. ***We recommend that the Government should use its planned public preparedness campaigns, such as the Be Ready campaign, to make resilience and practical readiness a normal part of everyday life, strengthening civic responsibility and psychological preparedness, and encouraging individuals and households to take sustained action to prepare for emergencies.***

277. ***We recommend that the Government use its Be Ready campaign to deliver clear public preparedness communications, working through trusted local networks and tailoring messaging to different groups, including young people, vulnerable people, and those whose first language is not English or Welsh. The Government should ensure that there is a sustainable pipeline of qualified Public Service Interpreters and translators to support this.***

278. ***We recommend that the Government should distribute a booklet to every household, modelled on the Danish and Swedish equivalents, providing practical guidance on what to do during a crisis and the support people can expect from national and local Government and local community responders. This should be complemented by a multilingual public preparedness app, modelled on Finland's 112 Suomi app, enabling people to contact emergency services with their location transmitted automatically, receive official warnings targeted to their area, and access guidance on preparing for and responding to emergencies.***

279. ***We recommend that the Government require local resilience arrangements to identify, maintain and publicise accessible local stocks of food, water and other vital products for people who require these. The Government should also help local Government to establish a volunteer system to deliver essential supplies directly to those who are unable to obtain them themselves because of distance, illness, disability or other barriers.***

---

439 Q 21 (Kristina Beckvard)
440 Q 18 (Stefan Gullgren)
441 Written evidence from Vival Corporation Ltd (NLR0009)
442 Q 208 (Angela Eagle MP)
443 Q 203, QQ 208–209 (Angela Eagle MP)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Collective mindsets

Community mindset

280. There was evidence that levels of resilience vary between communities. Councillor Boughton said that "some communities are much better prepared because they are much more alert to the risk than others".[444] VCSEP wrote that "exposure to national risk is uneven" and that "national preparedness messaging does not land evenly across communities".[445]

281. We heard examples of good practice on promoting resilience achieved by particular communities (see Box 4). One aspect of this was that communities should make use of the assets which they already have. Resilience Web CIC and Cambridge Room found substantial knowledge, activity and expertise already present within local communities.[446] The National Emergencies Trust proposed making preparedness tangible through familiar community buildings which already serve as trusted meeting places.[447]

Box 4: Community good practice

The 'How Resilient is Cambridge' project convened six hybrid events on food, reuse, flooding, energy, communications and community, bringing local and national experts together with councillors, community groups and residents. It identified expertise already present in the community, connected local organisations and enabled residents to raise issues directly with councillors.[448]

Horningsham Parish Council in Wiltshire brought together residents, volunteers, farmers, landowners, local institutions and voluntary organisations to test its emergency plan through a tabletop flooding exercise. The exercise identified strong community cohesion, detailed knowledge of local infrastructure and established informal support networks but also gaps in access to information and local co-ordination.[449]

The Greater Manchester neighbourhoods of Edgeley and Higher Folds worked with residents, councils and local voluntary organisations to co-design measures addressing flooding, extreme heat and underlying social vulnerabilities. In Edgeley, engagement with residents led to the development of a Resilience Hub, whose activities reached 300 residents with information about climate risks.[450] During flooding in 2020, Haydon Wick Parish Council operated as a multi-agency incident hub and provided refuge, food, donated clothing and continuing support while residents were rehoused. St Ives Town Council has established two volunteer-run Emergency Liaison Points which can be operational within an hour of activation.[451]

Through the Regional Community Resilience Group, which works across Northern Ireland's 11 councils, local authorities and community organisations have developed household and community emergency plans addressing severe

444 Q 6 (Councillor Matt Boughton)
445 Written evidence from the VCS Emergencies Partnership (NLR0061)
446 Written evidence from Resilience Web, CIC, Cambridge Room (NLR0074)
447 Written evidence from the National Emergencies Trust (NLR0114)
448 Written evidence from Resilience Web, CIC, Cambridge Room (NLR0074)
449 Written evidence from SafehousePro UK Ltd (NLR0030)
450 Written evidence from Resilient Cities Network (NLR0099)
451 Written evidence from the National Association of Local Councils (NLR0041)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

weather, flooding, power outages, fuel disruption and difficulties accessing services.[452]

282. Witnesses emphasised that communities should be involved in drawing up local emergency plans, not just in following them. Armagh City, Banbridge and Craigavon Borough Council described how "household and community emergency plans are developed with and by communities" in parts of Northern Ireland.[453] The Resilient Cities Network gave an example in which preparedness workshops produced a plan through direct resident participation rather than top-down design.[454]

283. Government representatives also recognised the contribution that voluntary, cultural and community organisations can make during emergencies. The Minister cited local food kitchens during the pandemic and said that central Government should support such initiatives.[455] Jonathan Martin said that the Government was keen to support cultural and sporting organisations which could provide space during emergencies.[456]

Government mindset

284. There was broad consensus that the Government tends to focus on short-term priorities. The Fairness Foundation referred to "the short-term perspective endemic in our politics".[457] The National Preparedness Commission said that the Treasury's Green Book, through which it assesses the costs, benefits and risks of proposed policies, could undervalue benefits arising many years in the future.[458] Sian Jones said that five-year spending cycles give departments insufficient incentive to plan over longer periods.[459] Fiona Hill CBE advocated "horizon-scanning of about 20 or 30 years", saying that Governments dealing with successive immediate crises struggle to undertake this task.[460]

285. Witnesses emphasised that shared and interconnected risks cannot be addressed by the UK acting alone. RAND Europe recommended that the Government undertake multinational engagement to address cyber, hostile-state, supply chain and climate risks.[461] Dr Neetesh Saxena said that since risks can cascade through trade, finance, technology and climate systems, UK preparedness needs "coordinated international intelligence sharing" and stronger international co-ordination.[462]

286. The Government said that it was seeking to strengthen its international cooperation. The Minister said: "We want to get best practice from as many of our NATO allies as we can".[463] Roger Hargreaves described mutually beneficial exchanges with France, the Netherlands and the Scandinavian

452 Written evidence from Armagh City, Banbridge and Craigavon Borough Council (NLR0122)
453 *Ibid.*
454 Written evidence from Resilient Cities Network (NLR0099)
455 Q 204 (Angela Eagle MP)
456 Q 183 (Jonathan Martin)
457 Written evidence from Fairness Foundation (NLR0155)
458 Written evidence from National Preparedness Commission (NLR0004)
459 Q 2 (Sian Jones)
460 Q 31 (Fiona Hill)
461 Written evidence from RAND Europe (NLR0139)
462 Written evidence from Dr Neetesh Saxena (NLR0016)
463 Q 210 (Angela Eagle MP)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

countries, adding that Ireland is "arguably our most important international partner on civil protection work".[464]

287. **Overall readiness remains inadequate and uneven across communities and sectors. There are examples of good practice, but too many businesses appear insufficiently engaged with national resilience imperatives. Decisions made by the Government and business continue to give insufficient weight to long-term systemic risks in favour of short-term priorities and convenience.**

288. ***We recommend that within six months of publication of this report, the Government should require each Local Resilience Forum to establish and maintain operational registers of suitable public and private buildings that can be used as shelters or community resilience hubs in the event of emergencies such as flooding or a prolonged power cut. These should record capacity, facilities, accessibility, and power arrangements, and identify local storage facilities holding critical food, water, medicines, and other vital products.***

289. **National resilience requires a fundamental shift in how the country understands and prepares for risk. Preparedness must become a national priority, embedded in the decisions and actions of Government, businesses, communities and individuals. The measure of success will not be the number of initiatives announced, but whether the UK is demonstrably better equipped to withstand disruption, protect its population and maintain the essential functions of society.**

464 Q 211 (Roger Hargreaves)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

APPENDIX 1: LIST OF MEMBERS AND DECLARATIONS OF INTEREST

Members of the National Resilience Committee

Baroness Coussins (Chair)
Baroness Curran (until 15 June 2026)
Lord Farmer
Baroness Helic
Baroness Hunter of Auchenreoch
Baroness MacLeod of Camusdarach (from 7 September 2026)
Lord Marland
Baroness Mobarik CBE
Rt Hon. the Baroness Northover
Lord Oates
Lord Peach KG GBE KCB DL
Baroness Paul of Shepherd's Bush (from 22 June 2026)
Rt Hon. the Lord Spellar
Rt Hon. the Baroness Winterton of Doncaster DBE (until 21 July 2026)

Declarations of Interests

Baroness Coussins

Co-chair of the APPG of Modern Languages, and Honorary President of the Chartered Institute of Linguists

Baroness Curran

No relevant interests to declare

Lord Farmer

Owner of a farm and employer of people on it

Shareholder, Tokamak (commercialisation of fusion energy)

Baroness Helic

No relevant interests to declare

Baroness Hunter of Auchenreoch

Shareholder, BP plc (energy)

Shareholder, Anglo American plc (mining)

Baroness MacLeod of Camusdarach

No relevant interests to declare

Lord Marland

Category 1: Remunerated employment etc.

Director, ICP Group Holdings Ltd, ICP Holdings Ltd and subsidiaries ICP General Partner Ltd and ICP Capital Ltd (insurance)

Participation in Lloyds underwriting through Insurance Capital Partners LLP

Director, Herriot Ltd (property, consultancy and investments)

Director, JP Marland and Sons Ltd (property, consultancy and investments)

Chairman, Commonwealth Enterprise and Investment Council Ltd

Chairman, EcoWorld Management and Advisory Services (UK) Ltd

Member of the Investment Advisory Committee, Kuwait Investment Authority

Director, Janspeed Technologies Ltd (manufacturer of motor parts)

Director, Five Rivers Eco Homes Limited

Director, Bspoke Insurance Group Ltd (formerly Pangaea Group Holdings Limited) (insurance)

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Chairman, UK General Insurance Ltd
Category 2: Shareholdings etc. (a)
Herriot Ltd (property, consultancy and investments)
Five Rivers Eco Homes Limited
J P Marland and Sons Ltd (property, consultancy and investments)
Test Match Extra.Com Limited
Category 2: Shareholdings etc. (b)
ICP Holdings Ltd (insurance)
EcoWorld Management and Advisory Services (UK) Ltd
Many Group Limited (formerly Bought by Many Ltd) (internet crowdsourcing to reduce insurance premiums)
Dynamo Restaurants Ltd
SSLP Group Limited (technology)
Zen Risk Ltd (information technology consultancy)
Janspeed Technologies Ltd (manufacturer of motor parts)
Minden Ventures Ltd (software development)
Screenhits Limited (television programme distribution)
UNI Products Inc (Beauty Products)
Category 3: Land and property
Five flats in London (two in SW1, one in SW6 and two in E14) from which rental income is received
Three apartments, Dinard, France
Two apartments, Switzerland
One house and one flat in Salisbury from which rental income is received and two residential properties in Salisbury area

Baroness Mobarik CBE
No relevant interests to declare

Rt Hon the Baroness Northover
No relevant interests to declare

Lord Oates
Chief Executive, UK Alliance to End Malnutrition and Hunger

Lord Peach KG GBE KCB DL
President, UK Armed Forces Reserve and Cadets
Chair, Defence Security and
Strategic and Global Advisor

Baroness Paul of Shepherd's Bush
Strategic Adviser, Pool Re (terrorism reinsurance)

Rt Hon the Lord Spellar
No relevant interests to declare

Rt Hon. the Baroness Winterton of Doncaster DBE
No relevant interests to declare

Specialist Adviser

Robert Hall
Co-founder and Executive Director of Resilience First Ltd (2018–22)

A full list of Members' interests can be found in the Register of Lords' Interests: https://www.parliament.uk/hlregister

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

APPENDIX 2: LIST OF EVIDENCE AND COMMITTEE ACTIVITY

Evidence is published online at: https://committees.parliament.uk/committee/832/national-resilience-committee/publications/

Evidence received by the Committee is listed below in alphabetical order.

Alphabetical list of witnesses

The ABI	NLR0129	
Accenture Cybersecurity		QQ 54–61, Oliver Neuberger, Managing Director
ADS Group Ltd	NLR0040	
The Alan Turing Institute	NLR0091	
Prof David Alexander	NLR0006	
All-Party Parliamentary Group on Modern Languages	NLR0112	
Dr Stuart Andrews	NLR0017	
Anonymous	NLR0005	
Prof Sotirios Argyroudis	NLR0063	
Armagh City, Banbridge and Craigavon Borough Council	NLR0122	
Audiebant Ltd	NLR0045	
Avioniq AB	NLR0031	
Michael Banahan	NLR0085	
Baroness Batters DL		QQ 116–124, Former President, National Farmers' Union
BBC		QQ 139–150, Rhodri Talfan Davies, Deputy Director General
HE Kristina Beckvard, Danish Ambassador to the United Kingdom		QQ 18–30
Bedfordshire Local Resilience Forum	NLR0130	
Dr Keith Bell	NLR0107	
Dr Bing Wu Berberich	NLR0034	
Bittium	NLR0116	
Jessica Bland	NLR0098	

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Simon Boor	NLR0007, NLR0159	
Simon Bradley	NLR0142	
Elisabeth Braw		QQ 62–70, Senior Fellow, Atlantic Council
Mr Gareth A. Brinkworth	NLR0098	
Brave Within LLP	NLR0067	
Prof Sarah Bridle	NLR0064	
British Armed Forces		QQ 78–91, Lieutenant General Sir Charles Collins KBE DSO, Deputy Chief of the Defence Staff Lieutenant General Paul Griffiths CB, Commander, Standing Joint Command
British Chambers of Commerce	NLR0140	
British Cleaning Council	NLR0043	
British Red Cross	NLR0056	
British Society for Antimicrobial Chemotherapy	NLR0015	
Broadcast2040+	NLR0042	
BT Group	NLR0141	QQ 139–150, Alex Towers, Director of Policy and Public Affairs
Stephanie Buller	NLR0077	
Business in the Community	NLR0166	
Gareth Byatt	NLR0104	
Cabinet Office	NLR0126	QQ 201–212, Roger Hargreaves, Director, Civil Contingencies Secretariat
Neil Cameron	NLR0020	
Capita	NLR0102	
Cemex	NLR0010	
Centre for Long-Term Resilience	NLR0095	

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Centre for Whole of Society Resilience	NLR0119	
Mark Chapple	NLR0108	
Chartered Institute of Linguists	NLR0028	
Chartered Institution of Highways & Transportation	NLR0084	
Cheong Ming Lam	NLR0008	
Robert Chris	NLR0080	
Citizens Advice	NLR0037	
Cityforum	NLR0149	
Climate Majority Project	NLR0109	
Coalition on Secure Technology	NLR0051	
Coastal Survival School	NLR0168	
CogitoPraxis Nederland BV	NLR0039	
Confederation of British Industry		QQ 10–17, Helena Coe, Policy Manager
Continuity Forum	NLR0049	
ControlAI	NLR0060	
Jan Conway	NLR0163	
Critical Supply Group	NLR0106	
Dr Hugh Deeming	NLR0160	
Defence Gardens Scheme Community Interest Company	NLR0158	
DeltaQuad	NLR0115	
Department for Culture, Media and Sport		QQ 180–189, Jonathan Martin, Director for Project Delivery and Major Events
Paul DiPaola	NLR0083	
Dräger	NLR0052	
Prof John Drury	NLR0025	
Prof Patrick Duggan	NLR0017	
Dame Angela Eagle MP, Minister of State for Security		QQ 201–212

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Early Studies		QQ 92–103, Alfred Malmros, Co-Founder
Earth Capital Nexus	NLR0128	
ECAPS AB	NLR0089	
Emergency Planning Society	NLR0118	QQ 40–53, Stephen Arundell, Vice Chair & Director
Emerging Risks Global	NLR0002	
Environment Agency	NLR0134	
Escode	NLR0113	
Fairness Foundation	NLR0155	
Michael Farnworth	NLR0164	
Ian Fox	NLR0001	
Dr Dolapo Fakuade	NLR0127	
Dr Anastasia Filippidou	NLR0144	
Foreign, Commonwealth and Development Office		QQ 213–224, Ben Fender, Director, Defence and International Security Directorate; Robbie Bulloch, Director, Overseas Territories and Polar Directorate
Dr Mary Fraser	NLR0018	
Future Resilience Forum	NLR0147	QQ 31–39, Fiona Hill CBE, Founder,
Garve and District Community Council	NLR0035	
Dr Joel C Gill	NLR0053	
Grand Challenge AI	NLR0105	
Anna Goodden	NLR0062	
Government Cyber Unit		QQ 54–61, Michael Brunton-Spall, Deputy Director of Cyber Services
HE Stefan Gullgren, Swedish Ambassador to the United Kingdom		QQ 18–30
Guy's Hospital		QQ 170–179, Dr Peter Gogalniceanu, Centre for Health Security
Dr Tom Hambley	NLR0046	

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Maryla Hart	NLR0101	
HE Tore Hattrem, Norwegian Ambassador to the United Kingdom	NLR0011	QQ 18–30
Deborah Haynes		QQ 62–70
Hazards Forum	NLR0092	
Dr Nathan Hazlehurst	NLR0012	
Becky Heginbotham-Blount	NLR0014	
Anthony Heron	NLR0027	
Dr Natalie Higham-James	NLR0069	
Dr Fiona Hill CMG		QQ 40–53
Historic England	NLR0123	
Dr Lara Houston	NLR0046	
Howden	NLR0044	
Byron Hyde	NLR0070	
Dr Maitland Hyslop	NLR0013	
Institute of Civil Protection and Emergency Management	NLR0096	
Institute of Strategic Risk Management	NLR0076	
Institution of Civil Engineers	NLR0038	
International Association for Resilience Analysis	NLR0066	
International Committee of the Red Cross (UK and Ireland delegation)	NLR0146	
Dr James Irvine	NLR0107	
ISACA	NLR0133	
ISC2	NLR0050	
IsEveryoneSafe Ltd	NLR0022	
Joint Civil Aid Corps	NLR0153	
Prof Aled Jones	NLR0046	
Róisín Jordan	NLR0033	
Dr Nikolai Kazantsev	NLR0098	

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Prof Stefan Kepinski	NLR0064	
Sardar Aftab Khan	NLR0003	
KBR	NLR0124	
Jacqueline Kilby	NLR0082	
Dr Nadiia Kopiika	NLR0063	
Deborah Lane	NLR0046	
Prof Tim Lang	NLR0145	QQ 116–124, Professor Emeritus of Food Policy, University of London
Dr Andrew McClelland	NLR0026. NLR0033	
Debbie Lewis	NLR0073	
LINK ATM Scheme	NLR0036	
Lloyd's Register Foundation	NLR0057	QQ 92–103, Nancy Hey, Director of Evidence & Insight
Local Government Association	NLR0117	QQ 1–9, Councillor Matt Boughton, Chair, Safer and Stronger Communities Committee
Edward Lucas		QQ 62–70
M&C Saatchi World Services	NLR0088	
Marcus Lions	NLR0075	
Dr William Matthews	NLR0059	
Paddy McGuinness CMG OBE		QQ 190–200
medConfidential	NLR0023	
Medicines UK		QQ 170–179, Mark Samuels, Chief Executive
The Met Office	NLR0120	
Prof Lee Miles		QQ 104–115, Professor for Resilience and Disaster Management, Bournemouth University Disaster Management Centre

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Ministry of Defence		QQ 78–91, QQ 213–224 Damian Johnson MBE, Director of Homeland Security QQ 213–224, Brigadier Ben Halsted MBE, Military Strategy Operations Centre
Ministry of Housing, Communities and Local Government		QQ 180–189, Zainab Agha, Director of Resilience and Recovery
Ed de Minckwitz		QQ 190–200
Dr Femke Mulder	NLR0072	
Muslim Charities Forum	NLR0111	
Dr Davide Natalini	NLR0046	
National Association of Local Councils	NLR0041	
National Audit Office	NLR0161	QQ 1–9, Sian Jones, Director of Value for Money; Mfon Akpan, Director of Financial and Risk Management Insights
National Emergencies Trust	NLR0114	
National Fire Chiefs Council	NLR0055	QQ 161–169, Alex Woodman, Chief Fire Officer, National Lead for Resilience
National Gas	NLR0103	
National Heat Risk Commission	NLR0087	
National Infrastructure and Service Transformation Authority		QQ 151–160, Margaret Read, Infrastructure Strategy and Policy Director
National Police Chiefs' Council	NLR0143	QQ 161–169, Mark Williams, Chief Officer
National Preparedness Commission	NLR0004	QQ 31–39, Lord Harris of Haringey, Chair
National Register of Public Service Interpreters	NLR0100	

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Network Rail		QQ 151–160, Martin Frobisher, Group Safety and Engineering Director
Baroness Neville-Jones DCMG PC		QQ 190–200
Hadley Newman	NLR0136	
NHS Supply Chain		QQ 170–179, Andrew New, Chief Executive Officer
John Nissen	NLR0081	
Nokia	NLR0166	
Finn O'Donnell	NLR0078	
Frank O'Donnell	NLR0078	
Ofcom		QQ 104–115, Nihal Newman, Director for Resilience and Cybersecurity
Offshore Energies UK	NLR0121	
Dr Justin Okoli	NLR0127	
OpenHorizon	NLR0162	QQ 151–160, Polly Copeman, Senior Vice-President
Overton Advisory	NLR0068	
Dr Katie J Parsons	NLR0086	
Prof Mark Pelling	NLR0072	
Prof Gianluca Pescaroli	NLR0072	
Pool Re		QQ 125–138, Jonathan Gray, Chief Underwriting Officer
Dr James Porter	NLR0062	
Portsmouth Historic Quarter Trust	NLR0154	
Pupils 2 Parliament	NLR0165	
PwC UK	NLR0094	
Prof Danny Ralph	NLR0072	
Ramboll	NLR0047	
RAND Europe	NLR0139	
Prof Nicola Ranger		QQ 125–138

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Re:Act		QQ 71–77, Lieutenant General Sir Charles Stickland KCB OBE, Chair
Rebalance Earth Venture Limited	NLR0097	
Red Thread Collective	NLR0110	
The Resilience Imperative	NLR0090	
UK Resilience Academy		QQ 1–9, Dr Eleanor Parker, Head of Training and Curriculum,
Resilience First		QQ 10–17, Rick Cudworth, Executive Director
Resilience Web, CIC, Cambridge Room	NLR0074	
Resilient Cities Network	NLR0099	
Royal Academy of Engineering	NLR0131	
Saatchi & Saatchi		QQ 92–103, Sam Wise, CSO
SafehousePro UK Ltd	NLR0030	
Prof Angelina Sanderson Bellamy	NLR0064	
Louise Sandher-Jones MP, Parliamentary Under-Secretary of State for the Armed Forces		QQ 213–224
Sandoz	NLR0125	
Ian Saunders	NLR0156	
Dr Neetesh Saxena	NLR0016	
Sazani Associates	NLR0021	
Scottish Government	NLR0169	
Second Front Systems	NLR0048	
The Security Institute	NLR0071	
Vsevolod Shabad	NLR0079	
Prof Duncan Shaw	NLR0033	
Neil Shearing	NLR0024	
Dr Elta Smith	NLR0064	

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Antony So	NLR0145	
Society of Chemical Industry	NLR0148	
Solar Energy UK	NLR0135	
St John Ambulance		QQ 161–169, Matt Killick BEM, Chief Operating Officer
Prof Stergios-Aristoteles Mitoulis	NLR0063	
Stone Federation Great Britain	NLR0150	
Sarah Strachan	NLR0046	
Sustain	NLR0152	
Dr Haniya Syed	NLR0138	
Dr Faith E. Taylor	NLR0053	
techUK		QQ 139–150, Sophie Greaves, Associate Director for Digital Infrastructure
Dr Benjamin Trump	NLR0072	
HE Teemu Turunen, Finnish Ambassador to the United Kingdom		QQ 18–30
UK Defence First	NLR0019	
Dr Francesca Vantaggiato	NLR0062	
Prof Liz Varga	NLR0032	
VCS Emergencies Partnership	NLR0061, NLR0151	QQ 71–77, Dr Carolyn Otley, Board Member
The Vegan Society	NLR0058	
Viasat UK	NLR0132	
Vival Corporation	NLR0009	
Prof Neil Ward	NLR0064	
Dr Edith Wilkinson	NLR0144	
Jane Wright	NLR0107	
Phillip Wood	NLR0065	
Thomas Woolmore	NLR0093	
Workforce Development Trust	NLR0029	

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Young Foundation	QQ 71–77, Emily Morrison, Director of Sustainability

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

APPENDIX 3: CALL FOR EVIDENCE

The House of Lords Select Committee on National Resilience was appointed on 27 January 2026 to consider national resilience, including the role of local resilience. It is chaired by Baroness Coussins and will report by 30 November 2026.

This inquiry will address the current context for preparedness and resilience, including the threats which the UK currently faces; how to achieve a whole of society approach in which everyone plays a role in achieving resilience; the interconnectedness of risks across different threats, sectors, countries, and timeframes; and strategic gaps which could be addressed, including in the private sector.

This is a public call for written evidence to be submitted to the Committee. The deadline for submissions is 10am on Monday 20 April 2026. The Committee is keen to hear from a diverse range of individuals and organisations.

Diversity comes in many forms and hearing a range of different perspectives means that committees are better informed and can more effectively scrutinise public policy and legislation. Committees can undertake their role most effectively when they hear from a wide range of individuals, sectors or groups in society affected by a particular policy or piece of legislation. We encourage anyone with experience or expertise of an issue under investigation by a select committee to share their views with the committee, with the full knowledge that their views have value and are welcome.

Questions

The Committee is seeking written submissions addressing any or all of the following topics. There is no need to answer every question.

Risk Assessment

(1) How far are national and international risks inter-connected, including across different sectors and across short-term and long-term risks, and what are the implications for the national approach towards preparedness and resilience?

(2) What national risks could have the most severe impact in a reasonable worst-case scenario, including nuclear accidents and loss of control of satellite communications?

(3) Since the 2025 Strategic Defence Review, what changes have there been to the national resilience implications of the geopolitical environment for defence spending, development of the country's industrial base, and military recruitment?

(4) What risks does the private sector face, including to cyber activity and supply chains, and how do these vary across key industries, such as finance, food, water, medicine, and transport?

Whole of Society Approach

(5) How can a shared vision be developed to improve preparedness and resilience across the whole of society?

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

(6) How can understanding of preparedness and resilience be improved, with action encouraged at all levels of society so that these priorities are both seen as relevant and achievable in practice?

(7) How can the preparedness and resilience of civil society be strengthened, such as through funding community organisations and the inclusion of people of all ages and from all backgrounds?

Communication and Information

(8) What does the public perceive to be the biggest risks, and how can communication help to provide information about these risks, including those that are already established or materialising, and support conversations about attitudes towards preparedness and resilience?

(9) What are the risks of disinformation concerning preparedness and resilience, including through digital channels and around elections, and how can these be mitigated, such as through the involvement of community organisations?

(10) How should communication concerning preparedness and resilience, including the national curriculum, be targeted for particular groups, including young people aged 11–17, students, and vulnerable people?

Cross-cutting Issues

(11) What barriers have there been to implementing improvements to preparedness and resilience, such as inaction, inappropriate structures, inadequate funding, and short-term thinking?

(12) What legislative measures should be considered to improve preparedness and resilience, such as a Defence Readiness Act and duties for organisations to incorporate resilience into their internal planning and business models?

(13) What lessons concerning preparedness and resilience can the UK learn from other countries, including Nordic countries, and how can it facilitate international co-operation on these issues?

(14) How were preparedness and resilience achieved in the past, such as during the Second World War, and what are the implications for the current environment?

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

APPENDIX 4: NATIONAL SITUATION CENTRE VISIT NOTE

On Tuesday 14 April 2026, the Committee visited the National Situation Centre at the Cabinet Office. During this visit Members received a private briefing on the UK's capability for using data in support of emergencies. Following the briefing Members had an opportunity to ask questions.

The National Situation Centre (SitCen) is the Cabinet Office's central data and analysis centre for crisis response and national resilience. It was established to give ministers and senior officials a quicker and clearer picture during a crisis of what is happening, what the likely effects may be, and where the main vulnerabilities are. It was set up in 2021 as part of the Integrated Review[465] and was informed by lessons learned from the Covid-19 pandemic.[466]

Government guidance says that the SitCen works closely with the COBR Unit and is the main mechanism through which data and analytical insight are brought together and presented to decision-makers in emergency scenarios.[467] The Institute for Government similarly describes it as a "key resource for COBR."[468]

The Government also stated that SitCen's data strategy is to map public and private sector data against National Security Risk Assessment risks.[469] It explained in its 2023 Resilience Framework that this supports more effective and rapid deployment of data during crisis response, as well as improving resilience by identifying and addressing data gaps.[470]

The Government stated that SitCen can produce short-notice analysis drawing on over 700 anonymised and aggregated datasets.[471] It also noted that SitCen can produce analysis for over 85% of risks identified in the National Security Risk Assessment, and that it has developed, with the Office for National Statistics, a Risk Vulnerability Tool to estimate the number of people vulnerable to selected risks.[472] It explained that the Risk Vulnerability Tool created by the SitCen and the Office for National Statistics is "accessible to officials in the UK government and the devolved governments through the SitCen's cross-government dashboard."[473]

The Government's Resilience Framework stated that the UK Government will work with Local Resilience Forums to strengthen data, intelligence and analysis capacity and capability. It noted that this would "support them to make the best use of data to target activity and measure success as well as being a vital tool in response and recovery."[474] It said that "ensuring appropriate sharing of UK Government data and information and building strong links with the National Situation Centre"[475] would be central to this.

---

465 Cabinet Office, *The Integrated Review 2021*, 16 March 2021
466 Cabinet Office, *The UK Government Resilience Framework*, 4 December 2023
467 Analysis Function, *Data sharing for national crisis response*, 14 August 2023
468 Institute for Government, *COBR (COBRA)*, 23 January 2020
469 National Security Risk Assessment (NSRA) is the main tool for assessing the most serious civil contingencies risks facing the UK. Cabinet Office, *The UK Government Resilience Framework*, 4 December 2023.
470 Cabinet Office, *The UK Government Resilience Framework*, 4 December 2023
471 Cabinet Office, *UK Government Resilience Action Plan*, 14 July 2025
472 *Ibid.*
473 Cabinet Office, *The Amber Book: Managing crisis in central government*, 28 April 2025
474 Cabinet Office, *The UK Government Resilience Framework*, 4 December 2023
475 *Ibid.*

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

APPENDIX 5: SCENARIO SIMULATION EXERCISE NOTE

On Wednesday 22 April 2026, the Committee took part in a three-hour war-gaming simulation exercise. Each Member was assigned the role of a Cabinet Minister within a simulated COBR meeting.

The exercise was facilitated through a White Cell and a Red Cell. The White Cell represented relevant elements of the civil resilience sector, the Armed Forces, intelligence services, the media and the public, and facilitated the exercise and recorded the decisions taken. The Red Cell represented a hostile state actor and introduced developments into the scenario to which participants were required to respond.

The scenario was set in 2028 and examined how the UK might respond to an escalating campaign of hostile activity directed against the UK and its interests. The activity was designed to place economic, political and societal pressure on the country, undermine public confidence and test national resilience.

The scenario was hypothetical. It was designed to explore plausible challenges that might arise during a period of heightened international tension and was not intended as an assessment of the likelihood of particular events occurring or of the intentions of any specific state.

The exercise consisted of two turns representing different stages of escalation. Hostile actions were largely pre-scripted, while Committee Members were able to propose responses that the UK Government could realistically take.

The first turn focused on sustained activity below the threshold of armed conflict. The challenges presented to Members included:

- cyber disruption affecting public and private-sector systems;
- sabotage and disruption affecting critical infrastructure;
- hostile activity affecting UK territorial security;
- interference with communications and other essential services; and
- the use of disinformation and hostile information activity to increase social and political tensions.

Committee Members considered a range of measures relating to public communications, engagement with Local Resilience Forums and other relevant organisations, the protection of critical infrastructure, transport and logistics, and wider national preparedness.

The second turn represented a significant escalation in the threat environment. Members were presented with simultaneous disruption affecting critical infrastructure, healthcare, transport and other essential services, together with threats to personnel and national security.

Committee Members considered how Government might maintain essential services, support affected sectors, protect critical infrastructure and manage competing demands on national resources during a major and potentially prolonged crisis.

The exercise was conducted over a single afternoon, whereas exercises of this nature may ordinarily take place over one or more days. The time available

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

therefore limited the extent to which participants could explore individual issues and the number of possible responses that could be considered.

The relatively small number of participants also meant that the exercise prioritised breadth over depth. Some areas were deliberately placed outside scope in order to allow Members to focus primarily on domestic national defence, preparedness and resilience.

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

APPENDIX 6: UNIVERSITY STUDENT ROUNDTABLE SUMMARY NOTE

Background

This note summarises the main themes raised during the roundtable that took place on 4 June 2026. It is not a transcript and does not attribute comments to individual students. The roundtable brought together 20 university students from across the UK, representing a diverse range of backgrounds, age groups and academic disciplines.

Key issues raised

Students were divided across three tables, which considered national resilience through government, business, local and personal lenses. Across the discussion, students repeatedly said that resilience needs to be explained in practical terms, linked to credible risks, and supported by clear actions that people, communities, businesses and public bodies can take before a crisis.

- Many students found the term 'resilience' too broad. 'Preparedness' was seen as clearer because it points towards action.
- Students were concerned about climate change, cyber-attacks, pandemics, loss of utilities, disruption to supply chains, energy costs, geopolitical risk, interference with technology and data, and misinformation.
- There was a strong view that public information should be clearer, easier to find, and provided before a crisis rather than only during one.
- Trust was a central theme. Students described mixed trust in Government and the media, strong concern about misinformation on social media, and a need for credible messengers.
- Local networks, including family, faith groups, charities, universities, councils and emergency services, were seen as important for identifying vulnerable people and reducing panic.
- Students supported practical volunteering and community action, but there was little appetite for compulsory military service or front-line military roles.

Themes from the discussions

Terminology and framing

Several students preferred the word 'preparedness' to 'resilience'. They felt that preparedness is easier to understand, less abstract, and more directly linked to what people need to do. By contrast, resilience was seen as a broad term that can mean different things depending on the context.

Some students said that resilience often sounds like an individual mindset rather than a national responsibility. Others linked national resilience with military threats, war, climate change or crisis response. This made the term feel large and difficult to act on.

There was also discussion of whether resilience should mean returning to the previous state after a crisis. Some students argued that the aim should be to 'bounce forward' by learning from shocks and improving the system, rather than simply restoring what existed before.

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Risks that felt most important to students

Students raised a wide range of risks, with climate change, pandemics, cyber-attacks and the loss of basic utilities mentioned repeatedly.

The experience of COVID-19 shaped many comments. Students referred to empty supermarket shelves, exposed supply chains and a sense that Government responses were often reactive. Some questioned whether the UK was ready for another pandemic.

Geopolitical risk was also raised. Students linked foreign affairs, technology, data security, overseas dependencies and cuts to international support with long-term resilience.

Trust, information and misinformation

Trust was one of the strongest themes. Students said they often rely on social media because it is fast, but they also recognised that it could spread misinformation quickly. Several students said they cross-check information with more established sources, official documents, university or library sources, or NHS information.

Views on the BBC and other news outlets were mixed. Some students said the BBC is more accurate on facts than many other outlets, while others felt it is less neutral than it once was. A common view was that all news has some perspective and that people need to compare multiple sources.

Students also discussed misleading headlines and algorithms. They noted that people may share or react to headlines without reading the full article, and that complex subjects such as climate change can be difficult for the public to understand unless the information is made accessible.

Government preparedness and public communication

Students wanted more transparency about credible risks without creating unnecessary fear. They recognised that Government may not want to alarm people, but felt that more honest and earlier communication would help people feel prepared rather than shocked when a crisis happens.

Awareness of existing Government preparedness material was low. In one group, only one out of eight students had heard of the Government's Prepare website. Students said that important information cannot rely only on a website that people may not know exists or may not choose to visit.

The emergency alert system was seen as useful and credible for urgent, life-saving action. However, students warned that it should not be used too often, because overuse could make it feel less urgent. They suggested a separate approach for routine preparedness education.

Local resilience, community networks and vulnerable people

Students saw local community hubs as essential. Family, neighbours, faith groups, charities, universities, councils, police, fire services and local representatives were all mentioned as possible parts of a trusted local network.

A recurring point was that local networks can identify who is vulnerable and offer support before panic develops. Students suggested that a clearer picture of local vulnerability would help communities know who may need help during a crisis.

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Students were particularly concerned about elderly and vulnerable people who may struggle with digital services. They called for better support in social care with more funding, better data, and accessible non-digital information.

Business, employers and critical sectors

Students discussed the role of businesses in national resilience. They argued that employers should invest in the resilience of their people, because the private sector covers a large part of the country and can make a significant difference during disruption.

Some students linked this to youth unemployment and access to opportunity. They suggested that the private sector should create more entry-level roles and opportunities for people with limited experience, because economic security and employment are part of wider resilience.

Students also discussed ways in which Government could encourage the private sector to take preparedness seriously. Suggestions included presenting resilience as a useful long-term investment, recognising good practice, using public procurement, and strengthening duties under the Civil Contingencies Act.

Several sectors were raised as important to resilience, including energy, water, food, utilities, technology and supply chains. Students were concerned about dependence on other countries, lack of visible engagement from utilities companies, and whether some companies are too focused on customer relations rather than resilience planning.

Education, skills and youth engagement

Students repeatedly suggested that preparedness should begin earlier in life. Schools, universities and local authorities were seen as useful routes for teaching practical skills and explaining local risks.

Examples raised included first aid, CPR, survival skills, household emergency planning, climate risk, flood risk, digital safety and how to identify reliable information. Some students noted that first aid and CPR had not been taught consistently at school.

Students were interested in examples from other countries where preparedness is taught or rehearsed in more practical ways. They said training could be made engaging if it was framed as useful and practical rather than frightening.

International comparisons and examples

Students referred to several international examples. Sweden's public information booklet on crisis and war was discussed as a possible model. Students felt a similar booklet could be useful if it was calm, practical and clear, although they warned against creating a culture of fear.

Taiwan was discussed in relation to public information, co-ordination between public bodies and rehearsed plans for action during a crisis. Students were interested in the idea of practical preparedness days or exercises that show people what to do.

The Netherlands was mentioned in relation to flood risk management and education. Nigeria was raised as an example from the pandemic, where students

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

referred to co-ordination between private and public sector interests in a gradual process.

Volunteering, service and practical participation

Students were generally supportive of volunteering and community-based action. They saw practical participation as a way to improve skills, strengthen local ties and support vulnerable people.

There was much less support for compulsory military service. Some students were open to non-front-line or support roles, but the stronger message was that young people were more likely to engage with voluntary, practical and community-based routes than with military framing.

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

APPENDIX 7: FINLAND VISIT SUMMARY NOTE

Background

This note summarises the main themes raised during the visit to Finland from 1 to 3 September 2026. It is not a transcript and does not attribute comments to individuals. Meetings were held with the National Emergency Supply Agency (NESA), army reserves, officials from the Ministry of the Interior, members of the Finnish Parliament, the National Defence Courses, and those responsible for security of supply and food security. We also visited a civil defence shelter in Kuopio to see how Finland's preparedness arrangements operate in practice.

Key issues raised

Across the visit, we heard that Finland treats security as a shared responsibility rather than the responsibility of one or two organisations. Preparedness is built in normal times, set out in law, supported by contracts with the private sector, and reinforced by a culture that people take part in from school onwards.

- Comprehensive security is described as a whole-of-society concept. We were told that a nation can only be resilient if it engages all stakeholders.
- Preparedness rests on three layers. A baseline of regulation, then contractual arrangements with companies, then voluntary activity.
- The National Emergency Supply Agency provides a shared threat picture and continuous analysis, and feeds information back to companies on where the gaps are.
- Finland has 50,500 shelters providing 4.9 million shelter spaces.
- Conscription and the National Defence Courses mean that people across government, business and civil society are used to working together.
- National resilience is treated as non-party-political, and the first responsibility of the state is understood to be security.
- Finland produces around 80% of its food domestically and holds grain reserves sufficient for nine months.
- Households are asked to hold 72 hours of supplies, and around half of Finns do so.
- Leadership was described in terms of co-ordination being in place rather than a single person being in charge.

Themes from the discussions

Comprehensive security and the whole of society approach

Finland uses the term comprehensive security to describe a whole of society model. Security is everyone's business and is not outsourced to one or two organisations. Officials said that a nation can only be resilient if it engages all stakeholders, and that continuous dialogue between government, the private sector and non-governmental organisations matters more than any single structure. This dialogue was described as ongoing rather than a one-off exercise.

This was presented as a long-term effort. We were told that security and preparedness cannot be solved quickly, because they depend on a mindset and a culture that develop over time. Every ministry has a director for security, or chief

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

of readiness, so that responsibility sits inside each department rather than only in one central body.

Clarity about the threat and honesty about consequences

A recurring theme was the need to be clear about the threat and then honest about the consequences. The statement of threat in the UK is unclear by comparison. Army reserves said it would be difficult for someone joining the British army to know what they were fighting for, and it was noted that the UK has no mandatory short military service.

Participants said the nature of threats has changed and that direct warfare is now part of the picture. Planning uses a total defence scenario of a prolonged conflict affecting supply chains. Finland also draws on international partners and has sought support from Swedish colleagues on air and maritime capability.

We heard that preparedness is not only a question of resources and money, and that everyone is responsible for their own preparedness. Finland has developed a constant state of preparedness rather than one that is switched on when a crisis arrives.

Regulation, contracts and voluntary arrangements

Preparedness in Finland is built in layers. There is a baseline of regulation, including a legal requirement on critical entities. The Rescue Act places a duty of care around fire and accidents. Building owners and occupiers, businesses and institutions have a self-preparedness obligation to prevent fires, protect people and property, carry out the rescue measures they can, and ensure safe evacuation. Specified sites must set this out in a written rescue plan, supervised by the rescue authorities. The Emergency Powers Act allows additional powers to be granted to authorities during emergency conditions, and only where their normal powers are not sufficient.

Emergency stockpiling operates in three ways. NESA maintains national emergency stockpiles, companies and other key operators carry compulsory stockpiling obligations set in law, and security stockpiling rests on agreements between individual companies and NESA. NESA holds no stockpiles of its own, and quantities are agreed with companies so the goods circulate as part of normal business. The Committee was told that NESA works with around 200 contracting partners, and that reserves are not drawn on while the market is still able to supply. Beyond these obligations, companies prepare largely on a voluntary basis, driven by business requirements, contracts with their own customers and risk management.

We were told that the EU has woken up to the challenges of security regulation, and that European level cooperation is needed alongside national measures.

Situational awareness and the shared threat picture

NESA provides a shared threat picture, situational awareness and analysis, and an updated understanding of the security situation. Information flows in both directions. The agency collects data from companies and shares back its assessment of where the gaps are and what needs to be done.

We heard that identifying vulnerabilities is the first step, and that restoring domestic capacity for certain critical products is an important part of the response. The preparedness system as a whole was described as a form of national insurance.

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

Civil defence and the shelter system

Civil protection authorities are responsible for civil defence and rescue services. This includes planning for wartime and the command-and-control system used to contact and direct rescue operations during conflict.

Finland has 50,500 civil defence shelters providing 4.9 million shelter spaces. Helsinki has around 600,000 residents and 900,000 shelter spaces. Anyone constructing a building above 1,200 square metres, whether a public or private entity, must include a shelter.

The owner of a shelter is responsible for maintaining it. Where a shelter is used for other purposes in normal times, and many are, as warehouses, sports halls or swimming pools, it must be possible to convert it to civil defence use within 72 hours. Equipment must be inspected and serviced at least every ten years, and the record produced to the rescue authorities on request. Training on shelters is provided by the regional rescue service organisations, and each property is expected to have someone who knows how to bring its shelter into use.

Rescue services draw on around 6,000 professionals and 14,000 volunteer fire brigade members, alongside third sector activity. The Emergency Services Academy has revised its curriculum in response to lessons learned.

In Finland, around 20% of military reservists are trained medics. In an emergency a decision is needed on whether they serve with the health service or complete their military service. In Finland this is decided in advance.

Leadership and co-ordination

Questions about leadership drew a consistent answer. There was constant reinforcement that it does not matter that there is no single person in charge, because what matters is that co-ordination is in place.

The Security Committee is a permanent body that assists the Government and ministries on comprehensive security. Its 20 members and four experts are drawn from across the ministries, the security authorities and the business community, and it is chaired by a Permanent Secretary from the Ministry of Defence, where its secretariat sits. It follows the security environment, coordinates proactive preparedness, oversees implementation of the Security Strategy for Society and the Cyber Security Strategy, and prepares statements and recommendations. It meets about once a month rather than only in response to events.

Conscription, the National Defence Courses and shared culture

National resilience in Finland is non-party-political, and that public private partnership and conscription together mean people are used to working with each other. This was described as a matter of culture and mindset.

The example given was the cutting of cables in the Baltic Sea. The public and private sectors began working together immediately. The cables are owned by private companies that compete with one another, but they shared data because it was in the interest of the country to do so, even where it was not in the interest of the individual company.

The National Defence Courses were described as a central part of this culture. Attendance is by invitation only, with a selection process once a year. The aim is to educate highly capable people in key positions, including chief executives,

STRICTLY EMBARGOED UNTIL 06:00 MONDAY 16 NOVEMBER 2026.
You must not disclose this document or its contents until the date and time above; any breach of the embargo could constitute a contempt of the House of Lords.

directors, non-governmental organisations and faith groups. Participants are taught about Finnish society, and the courses are said to change mindsets and build networks and connections. Those selected receive a badge, and selection is considered an honour.

The courses provide insight rather than classified information, and include briefings, discussions, visits and scenario-based exercises. The Ministry of Defence funds them at around 1 million euros a year. By the end of this year around 75% of members of the Finnish Parliament will have attended.

We heard that around 65% of the male population complete military service, although this figure is falling, which was attributed to mental health grounds. There is no mandatory conscription for women.

Security of supply and food

Security of supply is intended to ensure the continuity of society's critical functions, and Finland focuses on material preparedness.

Households are asked to hold 72 hours of supplies, on the basis that people would then be able to buy a further three days of food in stores. The guidance is to keep a rolling buffer of three days of the things a household normally uses, so that nothing goes out of date. A yearly survey found that around half of Finns hold three days of stock in line with the guidance.

Finland produces around 80% of its food domestically. Stockpiling requirements cover food grains, with reserves sufficient for nine months of use by the whole population, as well as seeds, plant production, fertiliser and raw materials. The same approach applies, with regulation as the baseline, then contract-based stockpiling with the private sector, then voluntary arrangements.

Work is under way on a resilient retail network. NESA's project, run with the grocery chains and since extended to fuel distribution, is building a network of around 300 shops designed so that in an emergency no one would be more than 50 km from an operating shop and fuelling station in a city, or 150 km in the countryside. Shops in the network would have their power secured by backup generators, with payment systems, communications and logistics chains covered as well.

Cyber security and the private sector

When discussing cyber security, several discussions reinforced that a country is only as strong as its weakest link. Guidance is available to companies and the government funds grants to encourage the private sector, and smaller enterprises in particular, to invest in cyber education and security

Misinformation, education and public information

Participants said that work on misinformation and disinformation begins at school. Phones are banned in schools, which was said to bring a number of benefits. Sovereignty was raised as part of the same discussion.

The 112 Suomi app, produced by the Emergency Response Centre Agency, is free and available to anyone with a mobile device. Calling the emergency number through it transmits the caller's exact location automatically. Since 2021 it has also been one of the statutory channels for public warnings, and it carries official warnings, public notifications and traffic alerts targeted to the user's region.