The Resilience Imperative:
Submission of Written Evidence to the House of Lords
National Resilience Committee

Date of Submission

20th April 2026

Authors

Alexandra Ryabov, Alice Charalambous, Archie Millet, Emily Claessen, Fausto Sassen-Blees, Robert Duff, Sebastian Wigg

Table of Contents

About The Resilience Imperative

Hostile state actors are engaged in a sustained campaign of hybrid activity against the United Kingdom. This form of conflict is not waged on traditional battlefields but within society itself, through election interference, disinformation, sabotage, cyber-attacks, and arson, all designed to disrupt daily lives and undermine national stability.

The Resilience Imperative is a non-partisan, not-for-profit initiative focused on mobilising the UK, across policy, private enterprise, and society, to recognise and respond to this hybrid activity. Led by Lady Olga Maitland, it brings together stakeholders from business and community engagement organisations to develop a shared understanding of the threat environment and strengthen collective commitment to national resilience and defence spending.

Our Core Priorities

- **Education**: Equipping the public with the knowledge required to identify and resist hybrid threats, close the threat perception gap, and foster informed vigilance through targeted media campaigns, digital content, and educational resources.

- **Cultivate a Whole-of-Society Contribution**: Building a public consensus on the necessity of increased defence investment and normalising broader citizen participation in national resilience, both civil and military.

- **Strengthen Critical National Infrastructure**: Partnering with industry groups to enhance the physical and cyber resilience of essential systems, with a focus on digital infrastructure and the energy supply chain.

- **Bolster Cyber and Digital Capabilities**: Promoting best practices and fostering collaboration to improve the nation's cybersecurity posture and digital resilience against state and non-state actors.

Executive Summary

- The UK is operating in an increasingly complex and contested risk landscape, where sabotage, cyber activity, disinformation, and political interference are used in combination to exert sustained pressure.

- The most severe risks in a reasonable worst-case scenario arise not from isolated incidents but from coordinated or overlapping disruptions to Critical National Infrastructure (CNI), particularly the energy system.

- Since the 2025 Strategic Defence Review, the already elevated threat environment has continued to intensify, exposing capability gaps and insufficient defence and resilience investment needed to address both traditional and hybrid threats.

- Public awareness of hybrid threats is lacking, and the mental resilience, trust, emergency capability, and household preparedness remain insufficient to support an effective societal response.

- Understanding of the threat environment must be strengthened to build a mandate for defence and resilience investment through targeted communication and education.

Introduction

The submission highlights the systemic and evolving nature of contemporary risks, particularly those arising from hybrid threats, and demonstrates how coordinated disruptions could challenge existing resilience frameworks and lead to cascading impacts across society. It also examines the role of disinformation and societal resilience, and addresses public perception, communication strategies and targeted engagement. In doing so, it aims to support the National Resilience Committee's inquiry by identifying key gaps in current approaches and setting out practical recommendations to strengthen the UK's capacity to anticipate, respond to and recover from disruption in an increasingly complex and hostile environment.

The analysis is informed by a combination of open-source intelligence and intelligence-led insight, supported by our partnerships with Sibylline and Stonehaven, whose reporting on UK and European resilience trends and societal resilience survey together inform the evidence base of this submission. This is complemented by government publications, academic research, and case studies of recent incidents affecting European CNI.

The submission is structured in line with the Committee's questions:

- **Section 1: 'Risk Assessment'** examines the interconnected nature of national and international risks, assesses the most severe impacts in a reasonable worst-case scenario and looks at the current state of UK defence capabilities.
- **Section 2: 'Whole-of-Society Approach'** explores how resilience can be strengthened across society, including the role of community engagement and the risks posed by disinformation.
- **Section 3: 'Communication and Information'** considers public perceptions of risk and the importance of targeted communication in improving preparedness across different groups.

Responses to Questions

1. Risk Assessment

1.1 How far are national and international risks interconnected, 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?

The interconnections between national and international risks are clearly demonstrated by the hybrid warfare tactics currently targeting the UK. The UK has faced persistent cyber-attacks from Russian-aligned hacktivist groups directed at government departments, local authorities, and CNI, including attempts to disable online services and overwhelm public systems. These activities form part of a coordinated and centrally directed campaign of hybrid war conducted by Russia against the UK and its allies. Cyber-attacks represent only one element of a broader strategy that employs sabotage, disinformation, electoral interference, and economic pressure to undermine national resilience and public institutions.

Russia views these tools as interconnected and mutually reinforcing, all serving the same objective: to destabilise the UK and its allies, deter the UK from playing a leading role in Europe and providing sustained support to Ukraine, and to weaken the UK's ability to respond coherently to Russian actions. Hybrid tactics also exploit longer-term vulnerabilities such as energy dependency or political polarisation, creating a feedback loop in which short-term shocks deepen systemic fragilities, deliberately blurring the line between peace and conflict.

In light of this, we set out the following recommendations:

- First, governments must move beyond siloed thinking and recognise that risks to energy, health, infrastructure, and security are interconnected and require management across the whole of society, encompassing public services, private sector actors, and communities.

- Second, the international dimension of risk requires sustained cooperation. Threats originating beyond national borders cannot be addressed in isolation; effective resilience depends on information sharing across borders, coordinated planning, and collective action with allies and partners.

- Third, resilience must be both immediate and long-term. It involves not only responding to disruption but anticipating, adapting, and recovering amid continuous pressure. This includes strengthening infrastructure, reducing strategic dependencies, and enhancing societal cohesion and public confidence.

The boundary between peace and conflict has become less clear, and disruption is now persistent. Preparedness cannot be reactive or confined to crises; it must be embedded, collective, and continuous, ensuring that societies can withstand, adapt to, and operate through ongoing uncertainty.

1.2 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?

Building on the theme of interconnectedness and CNI, the national risks that could have the most severe impact in a reasonable worst-case scenario are not single incidents but a coordinated or overlapping set of cyber and physical attacks across the energy system's CNI, designed to degrade generation, transmission, control systems and recovery.

The UK's energy system is becoming increasingly interconnected, digitised and dependent both on distributed and geographically isolated infrastructure, as renewables technologies, namely offshore wind, remote operational technologies, and smart grids, expand. At the same time, electricity underpins all other essential services, and with the recent surge in demand for data centre projects, there is increased pressure for grid connections and greater energy security.[1]

The 2025 National Risk Register (NRR) emphasises this interdependence. It notes that failure of the electricity system could severely disrupt all other critical systems and that a nationwide loss of power would generate secondary impacts across telecommunications, water, sewage, fuel and gas.[2] However, the NRR assesses these risks primarily through individual reasonable worst-case scenarios, each centred on a single risk (e.g. a cyber-attack on electricity infrastructure, gas disruption, telecoms failure). While these scenarios incorporate cascading effects and, in some cases, multiple contributing causes, they are not designed to model concurrent or coordinated multi-risk events.

[1] Sibylline, *UK-Ireland National Resilience Monitor: Tracking the Threats Undermining Stability and Resilience*, (26 February 2026).
[2] HM Government, *National Risk Register 2025*, p.44. Available at: https://assets.publishing.service.gov.uk/media/67b5f85732b2aab18314bbe4/National_Risk_Register_2025.pdf

The assessment and preparation for these coordinated events are vital, given that the contemporary threat environment is already characterised not only by singular but by coordinated hybrid tactics, including synchronised cyber activity and the physical disruption of systemic vulnerabilities across European CNI.

To illustrate the type of attack the UK could face, on 29 December 2025, Poland experienced a series of coordinated Russian cyber-attacks targeting its energy sector. These attacks affected at least 30 wind and solar farms, a combined heat and power (CHP) plant serving nearly half a million customers, and a private manufacturing company. While electricity generation was not directly disrupted, and the attack on the CHP plant did not achieve its intended effect of interrupting supply, the incidents resulted in a loss of communication between facilities and distribution system operators. Crucially, they demonstrated the ability of a single threat actor to gain access to internal networks within power substations and conduct longer-term data exfiltration.[3]

In such a context, the most plausible high-impact scenario is not a single catastrophic attack, but a series of closely timed disruptions that:

- occur across different parts of the energy system
- degrade visibility, control and response capacity
- and overlap sufficiently to create simultaneous system stress.

Perfect simultaneity is not required. From a resilience perspective, overlapping disruption windows, with attacks occurring over hours, days, or weeks, are sufficient to overwhelm response systems and produce cascading failure. A deliberate staggering of attacks, designed to sustain prolonged pressure on emergency and government responses, could expose additional vulnerabilities over time. These weaknesses may then be exploited through subsequent targeted operations, whether cyber, physical or psychological, amplifying disruption and potentially inciting civil unrest.

If such an attack were to materialise, its impact would reach far beyond the energy sector. Immediate effects would include generation loss, grid instability, regional or national outages, and prolonged restoration challenges. The most severe consequences, however, would arise from cascading disruptions across interconnected systems, including telecommunications, fuel distribution, water and wastewater services, transport, emergency response and healthcare delivery. These secondary impacts, particularly the disruption to essential services and human welfare, pose the greatest risk to the UK and could, if prolonged or widespread, erode public confidence, heighten anxiety, and contribute to civil unrest, especially during winter, periods of constrained supply, or heightened geopolitical tension when resilience is already strained.

[3] CERT Polska, *Energy Sector Incident Report – 29 December*, (30 January 2026), p.4-5. Available at: https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

The Government's forthcoming Energy Resilience Strategy (ERS) represents a significant opportunity to ensure the UK's approach to energy resilience fully reflects the complexity of these modern, system-level risks. The next step is to operationalise its insight into stronger public-private partnerships, greater investment, and improved cross-sector collaboration and information-sharing.

In light of this, we set out the following recommendations:

- First, stronger central coordination of energy resilience is needed, including through designated lead authorities, formalised public–private partnerships, and cross-sector structures to support joint exercises, improve crisis response protocols, and identify systemic vulnerabilities. Currently, responsibilities for energy resilience remain distributed across government, regulators, and industry, risking gaps in oversight and limiting system-wide stress testing.[4] The Government's increasing emphasis on public–private cooperation and cross-sector collaboration ahead of the forthcoming ERS is a positive step towards improving crisis preparedness, and it must be effectively translated into practice.

- Second, this coordination should be complemented by greater investment in both pre-emptive resilience and rapid degradation management and recovery, including secure backup communications, restoration readiness, spare equipment strategies and manual fallback options where feasible. Resilience will depend both on preventing disruption and developing systems that can contain, isolate and restore under conditions of concurrent stress.

- Third, the UK should strengthen intelligence sharing and incident reporting across energy CNI, including operational-specific (OT) threat data, and near-miss reporting. Underreporting and fragmented visibility currently limit the ability to detect systemic risks before they materialise. The Polish case study illustrates the value of this approach: the subsequent report by CERT Polska provided a detailed technical analysis of the attack, including how vulnerabilities in remote access systems were exploited, and enabled wider sectoral learning. The UK should replicate this model of timely and technical reporting, whether publicly or within trusted channels, to identify vulnerabilities and anticipate threats. This should also be supported by public–private roundtables to share intelligence, identify trends, and embed best practices across sectors.[5]

[4] Sibylline, *UK-Ireland National Resilience Monitor,* (26 February 2026).
[5] CERT Polska, *Energy Sector Incident Report – 29 December*, (30 January 2026).
The Alan Turing Institute, *Enhancing the Cyber Resilience of Offshore Wind*, (Centre for Emerging Technology and Security, June 2024), p4. Available at: https://cetas.turing.ac.uk/publications/enhancing-cyber-resilience-offshore-wind

1.3 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?

Since the release of the Strategic Defence Review (SDR) in June 2025, the geopolitical environment has continued to escalate in ways that expose critical gaps in the UK's preparedness and military capability. The UK is underprepared to tackle the hybrid warfare threats identified in the SDR; cyber-attacks, disinformation, sabotage, and interference with CNI has accelerated.

The nature of warfare has evolved significantly. Hybrid threats now target the everyday functioning of civilian life instead of remaining confined to military targets or assets. These threats impact energy grids, undersea cables, supply chains, and digital infrastructure. A population that does not understand the nature of these threats cannot meaningfully participate in the national response. Awareness and preparedness at the societal level must go hand in hand with the critical increase in military capability.

Since the SDR, specific capability gaps have brought the UK's vulnerabilities under a magnifying glass. The Royal Fleet Auxiliary vessel Proteus remains the country's sole multi-role ocean surveillance ship with underwater monitoring capabilities, representing a single asset responsible for thousands of miles of vital seabed infrastructure.[6] Meanwhile, a legislative gap around drone countermeasures leaves the Armed Forces and civilian infrastructure operators in an ambiguous legal position when confronted with immediate aerial threats.[7] These are not isolated examples but reflect a broader pattern: the UK has acknowledged the shape of modern threats without yet substantially fielding the response those threats demand. With approximately 95% of UK imports arriving by sea, any sustained disruption to maritime routes or undersea cables could have immediate, cascading consequences for supply chains and everyday life. [8]

The above challenges, coupled with a further capability gap not yet remedied by increased military spending, have created a skills shortage in cyber, engineering, and manufacturing, threatening both military readiness and industrial resilience.[9] Defence spending in and of itself cannot alleviate the hybrid threat we are facing. The lack of specialised labour and societal understanding is equally a core problem when tackling the future of defence.

In light of this, we set out the following recommendations:

---

[6] Sibylline, *UK-Ireland National Resilience Monitor: Tracking the Threats Undermining Stability and Resilience*, (12 February 2026).
[7] Sibylline, *UK-Ireland National Resilience Monitor,* (12 February 2026).
[8] Department for Transport, "Transport Statistics Great Britain: 2022 Summary", (GOV.UK, 15 December 2022). Available at: https://www.gov.uk/government/statistics/transport-statistics-great-britain-2022/transport-statistics-great-britain-2022-summary
[9] UK Parliament, "Skill Shortages in the Armed Forces inquiry", (12 September 2018). Available at: https://committees.parliament.uk/work/3940/skill-shortages-in-the-armed-forces-inquiry/publications/

- First, the need for increased defence and resilience investment is clear, but it must be targeted and address modern domestic threats. For example, gaps in areas such as undersea surveillance, counter-drone measures and resilient CNI infrastructure, alongside the skilled workforce required to support them, should be closed to reduce vulnerability and limit the impact of disruption to society.

- Second, this investment must be underpinned by a stronger public mandate. Greater awareness is needed of the role defence and resilience spending plays in maintaining the safety and functioning of everyday life, from hospitals and emergency services to energy and communications. Building a public mandate for increased defence spending requires linking investment to protection against threats at home, rather than viewing it solely as funding for conventional military operations abroad.

2. Whole of Society Approach

2.1 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?

Disinformation poses a significant and growing threat to national resilience and preparedness, particularly in digital environments and during elections. This threat is increasingly understood in terms of "Cognitive Warfare", which, according to NATO, treats the human mind as a battlefield, using disinformation, social media, and psychological operations to alter perceptions, influence decision-making and break down societal trust.[10]

Hostile actors, in particular Russia, use Cognitive Warfare, not only to promote a political narrative, but also to advance opposing viewpoints simultaneously to amplify division and weaken institutional legitimacy. For example, during the Black Lives Matter (BLM) protests, Kremlin-linked bots posed both as anti-BLM activists, calling for the harsher policing of protests, and as BLM activists inciting rioting and more violent protests.[11] This "divide and amplify" approach is particularly effective on emotionally salient issues such as immigration, public health, and climate policy, where it fragments public discourse, generates domestic crises, and undermines trust in national institutions.

During elections, nations like the UK become even more vulnerable to Cognitive Warfare. Before the Brexit Referendum and the 2024 general election, significant spikes in disinformation were

[10] NATO OTAN, "Cognitive Warfare". Available at: https://www.act.nato.int/activities/cognitive-warfare/
[11] Denise Clifton, "Russian Trolls Stoked Anger Over Black Lives Matter More Than Was Previously Known", (Mother Jones, 30 January 2018). Available at: https://www.motherjones.com/politics/2018/01/russian-trolls-hyped-anger-over-black-lives-matter-more-than-previously-known/

reported.[12] The risk is twofold: disinformation may influence voter perceptions, and it may also undermine confidence in the integrity of the electoral process.

A further challenge lies in the self-reinforcing nature of disinformation ecosystems. Techniques such as microtargeting, artificial amplification, and repetition increase the persistence of false beliefs and make correction difficult. Reactive responses are therefore insufficient; resilience requires preventative measures.

In light of the above, we set out the following recommendations:

- First, the Government should set clear expectations for digital platforms, including biometric authentication, greater transparency around algorithms, and support for independent fact-checking. These measures must be clearly communicated to the public as a prevention of foreign interference and not as interfering with freedom of expression. Further, "Prebunking", a strategy to combat misinformation on social media, must be used by teaching users how to spot manipulation tactics before they encounter false content. Digital literacy workshops could take place in the community, employment, and education sectors, especially with government initiatives.

- Second, by fostering media literacy, acting as trusted local intermediaries, and facilitating dialogue across differences, Government bodies and community organisations should play a critical role in countering polarisation and strengthening social cohesion. Unlike depersonalised social media contexts, which algorithmically reward more extreme comments, community projects can enhance respectful dialogue and national trust through collaboration.[13]

3. Communication and Information

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

The public overestimates risks which are media-amplified, such as terrorism and plane crashes, while dramatically underestimating slow-burning, systemic threats like infrastructure failure and societal fragility. Effective communication does not just transfer information, it must bridge the

[12] Dr Marco Bastos, "Social media 'bots' used to boost political messages during Brexit referendum", (City St Georges, University of London). Available at: https://www.citystgeorges.ac.uk/research/impact/case-studies/social-media-bots-used-to-boost-political-messages-during-brexit-referendum

[13] Elizaveta Konovalova, "How social media platforms fuel extreme opinions and hate speech", (Warwick Business School, 20 March 2024). Available at: https://www.wbs.ac.uk/news/how-social-media-platforms-fuel-extreme-opinions-and-hate-speech/

gap between perceived and actual risk, build trusted relationships, and activate public preparedness behaviours.

Risk perception is shaped more by emotion, identity, and social environment than by probability or severity. The UK faces a widening preparedness gap: the 2025 NRR identifies threats from Cyber-attacks and extreme weather to societal instability and biological hazards, yet public awareness of these risks remains low, as does behavioural preparedness. A problem which compounds this is a lack of institutional trust; declining confidence in government and media means that official risk messaging is ignored or discounted, particularly among younger and more economically disadvantaged demographics.

The Cabinet Office's *UK Public Survey of Risk Perception, Resilience and Preparedness* (2025) exposed the scale of the awareness-action gap.[14] Two-thirds of respondents expected emergencies to increase over the next decade, yet only 19% were signed up for alerts or warnings, and just 10% were active in a community preparedness group. More telling still, 86% said the Government should bear primary responsibility for preparedness, while only 30% felt they themselves should.

Stonehaven's *Will and Preparedness Index* (2026), developed in partnership with our organisation, reinforces this pattern.[15] The Index assesses societal resilience across five core areas: threat awareness, mental resilience, trust in others and institutions, emergency response skills, and household preparedness. The findings show that the UK records an overall "Will and Preparedness Index" score of 50/100, placing the country in the "D" band of the index grading framework. In practical terms, the rating indicates limited societal resilience, with clear gaps in preparedness, psychological readiness, and a lack of response capability across the population.

If these vulnerabilities are not addressed, the public will continue to lack agency, community infrastructure, or the behavioural habits needed to respond effectively. This will increase economic costs, social fragmentation and mortality rates, while also deepening distrust in institutions at exactly the moment when a coordinated response is needed most.

In the light of this, we set out the following recommendations:

- First, communication strategies must shift from warning to activation, moving beyond disclosing risks and toward behaviour-enabling actions which frame preparedness as ordinary, achievable, and community-connected rather than fear-driven. Central to this is investing in trusted intermediaries, such as GPs, schools, faith leaders, and local authorities, which carry significantly more communicative trust than central government. Risk

[14] GOV.UK, "UK Public Survey of Risk Perception, Resilience and Preparedness: 2025", (23 July 2025). Available at: https://www.gov.uk/government/statistics/uk-public-survey-of-risk-perception-resilience-and-preparedness-2025
[15] Stonehaven, *Will and Preparedness Index*, (24 March 2026).

communication should be co-designed and distributed through these networks rather than being broadcast from the top down.

- Second, scenario literacy needs to become a civic norm at a societal level. Regular public-facing exercises, modelled on approaches in Sweden, Finland and Switzerland, for instance, should be embedded in everyday life to build the mental and physical resilience skills needed to recognise, respond to and mitigate risks before crises occur.

3.2 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?

Effective communication on preparedness and resilience must be strategically tailored to reflect the differing needs, capacities, and contexts of specific groups. A segmented approach, as opposed to a universal model, is essential to ensure that messages are catered to. This is particularly important when addressing young people aged 11–17, students in further and higher education, and vulnerable populations.

For young people aged 11–17, preparedness and resilience should not be treated as abstract concepts but integrated into subjects such as geography, science, and citizenship education. Teaching should emphasise real-world application through interactive methods, including scenario-based learning, simulations/workshops. This age group responds well to digital platforms, including social media and educational apps, which should be utilised to reinforce key messages in formats that align with how young people consume information. Peer-led initiatives, such as student ambassador programmes, can also strengthen engagement and promote a culture of shared responsibility.

For students in further and higher education, communication should reflect their increasing independence and capacity for critical thinking. In practice, this means equipping students with the skills to assess information related to risk and resilience. Students should be helped to distinguish between reliable information and misinformation and understand the origin and potential bias of content in digital environments. Communication strategies should encourage the use of multiple sources, enabling students to cross-reference information and engage with a diversity of perspectives. In addition, students should be encouraged to reflect on their own assumptions and beliefs. This includes building the ability to revise views in light of new information, which is essential in rapidly evolving crisis situations.

Learners at this stage are particularly receptive to new information and adaptable in their thinking, placing them in a strong position to develop these skills. Embedding these skills within preparedness communication not only improves immediate understanding of risks but also supports the development of responsible individuals.

Furthermore, Universities and colleges should incorporate preparedness into induction programmes, ensuring that students are aware of risks and know how to respond in emergencies. Communication channels such as campus apps and virtual learning environments are effective for this group and should be used consistently. In addition, there is value in linking resilience to employability and life skills. Workshops on first aid, crisis management, and mental resilience can provide practical competencies that extend beyond academic study. Encouraging student participation in volunteering, research, and partnerships with emergency services can also foster a proactive and informed student body.

For vulnerable populations, including older adults, people with disabilities, those from low-income backgrounds, and individuals with limited English proficiency, communication must prioritise accessibility, clarity, and trust. Information should be provided in multiple formats, including large print, audio, and easy-read versions, as well as in relevant community languages. Messaging must be clear and focused on actionable steps, avoiding technical or overly complex language. Trusted intermediaries play a crucial role in reaching these groups. Partnerships with local authorities, healthcare providers, charities, and community organisations are therefore essential. In some cases, more personalised approaches, such as community outreach or face-to-face engagement, may be necessary to ensure understanding and inclusion.

Across all groups, several overarching principles should guide communication efforts. Consistency of messaging across national and local levels is critical to avoid confusion. Repetition and reinforcement are necessary to ensure that preparedness becomes embedded in everyday awareness, rather than only considered during crises. This is something that is applicable to all groups. Communication should also be two-way, allowing for feedback and adaptation based on the needs of different communities. Finally, behavioural insights should inform the design of messages, ensuring they are not only informative but also effective in prompting action.

Targeted, inclusive, and practical communication strategies are essential to building a resilient society. By aligning content, delivery methods, and engagement strategies with the specific needs of different groups, preparedness can be meaningfully understood and effectively implemented.

Conclusion

The evidence presented above highlights that a whole-of-society model is essential. This includes not only investment in infrastructure and capability, but also sustained efforts to improve public awareness, trust, and participation in preparedness efforts. Communication strategies must also support behavioural change and ensure that individuals and communities are equipped to respond effectively to crises.

The Resilience Imperative exists for exactly this purpose: it aims to equip the public with an understanding of the current threat environment, how it affects daily life, and why increased and better-targeted defence spending is essential to protecting national security and our

values. Embedding this approach is critical to ensure the UK can anticipate, withstand, and recover from increasingly complex and sustained forms of disruption.