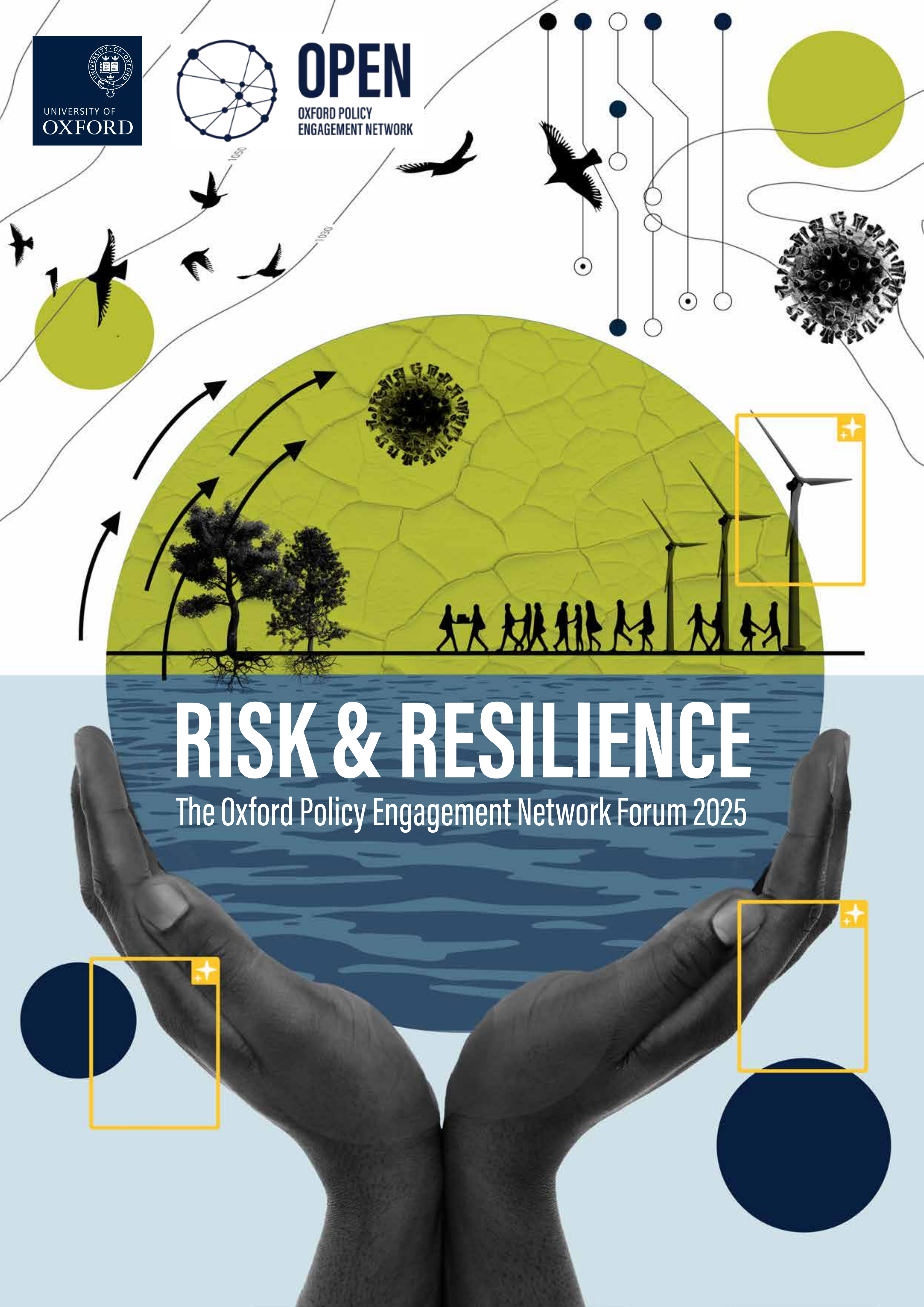
UNIVERSITY OF
OXFORD

OPEN
OXFORD POLICY
ENGAGEMENT NETWORK



RISK & RESILIENCE

The Oxford Policy Engagement Network Forum 2025

About OPEN

The Oxford Policy Engagement Network (OPEN) enables research and policy professionals to join forces in shaping public policy that protects what is valuable and changes the world for the better. Since its launch in 2020, the network has grown to include research professionals and students in more than 50 departments and faculties, as well as policy professionals in Oxford, across Whitehall and the UK, and around the world, who share our vision of public policy powered by the world's best available research evidence and expertise. We are committed to making more of policy professionals' expertise and to creating new ways, such as the OPEN Forum, for policy professionals to engage with the University.

You can find out more about our work at www.ox.ac.uk/open.

Contents

Introduction

How can the UK become more resilient? What can we do to better understand, anticipate, prevent, and respond to some of the major risks affecting the country? On 24 June 2025, more than 90 experts from government, industry and academia convened to tackle these questions. They focused on risks related to the environment and energy, human health and technology, and explored in depth specific challenges relating to each, evidence and tools that could help tackle them, as well as evidence gaps and avenues for potential collaboration.

This inaugural Oxford Policy Engagement Network (OPEN) Forum was hosted at the Blavatnik School of Government, in collaboration with the Oxford Martin School, Pandemic Sciences Institute, the ZERO Institute, with support from the University's Policy Engagement Team.

Policy professionals from more than 10 government departments and agencies were joined by those from Oxford City and Oxfordshire County Councils, businesses, and funders, as well as research professionals from numerous universities and institutes in life, medical, physical, and social sciences, as well as the humanities.

Following a welcome from the Dean of the Blavatnik School of Government, the Director of the Cabinet Office Briefing Rooms Unit addressed an opening plenary, providing an overview of some of the latest developments in the government's approach to risk and resilience.

The Chief Operation Officer of the School of Government led a discussion outlined the three main sub-themes. Participants then dispersed into three streams, one focused on each sub-theme, to pursue an agenda co-developed by academic and policy leads for each stream.

Participants reconvened for a closing plenary, introduced by the Director of the Oxford Martin School, and a panel discussion led by the Coordinator of the Crisis Management Programme at the Blavatnik School of Government, reflecting on key points arising in each stream and possible areas for future action, and some cross-cutting issues.

This report is intended as a resource for participants, other research and policy professionals, and funders. It summarises proceedings in the three streams and offers some suggestions for further reading. It draws on input from individual participants and groups but does not necessarily reflect the preferences or policies of any individual participant or organisation.

Energy & Environment

The UK has adopted a legally binding commitment to reach net zero by 2050. With over 80% of the UK's territorial greenhouse gases responsible for climate change coming from the use of energy, the transition to a zero-carbon energy system is the foundation for a stable climate.

The task of getting a zero-carbon energy system is urgent, yet also increasingly challenging. Ambitious targets are the starting point, but their delivery rests on effective implementation. Within the UK, continued progress towards its net-zero targets hinges on increasing the ambition of its climate change mitigation actions. While often a leader in global climate conversations, the UK's progress has also been undermined by inconsistent messaging and actions.

At the same time, continuing global warming and the increasing rate and magnitude of associated climate risks show that the UK must urgently build its resilience to climate change, particularly in its energy system.

Energy system resilience can be organised around three interrelated pillars: demand reduction and flexibility, storage, and low-cost renewable generation. Energy demand provides an important entry point. As the UK's economy decarbonises and multiple economic sectors are electrified, lowering energy demand and improving the efficiency of energy use will be crucial for achieving net zero, decreasing environmental impact, and reducing energy costs.

A key component of managing energy demand lies in the building stock. Much of the UK's built environment is among the oldest in Europe, possibly among the oldest in the world, and is therefore ill-suited to the demands of a changing climate. A timely policy response must channel new investments into technology and develop new energy demand policies, particularly targeting heating, cooling, and shifts in consumer behaviour, while ensuring a high quality of life for the UK's residents.

Another pillar of energy system resilience is storage. As the electricity system transitions to a high share of intermittent renewables, the UK will need large-scale electricity storage to manage system resilience and end its dependence on carbon-intensive fuels. This challenge extends far beyond the UK's borders: similar storage needs are emerging globally as countries pursue net-zero targets, creating both competitive pressures and export opportunities for British innovation. Determining which technologies can meet these requirements, and at what costs, is necessary to evaluate how policy can best accelerate implementation at scale.

Renewables offer the third pillar. In July 2024, the UK Climate Change Committee concluded that 'British-based renewable energy is the cheapest and fastest way to reduce vulnerability to volatile global fossil fuel markets.' At the same time, leveraging the multiple benefits offered by renewable energy entails unique challenges. In addition to switching to renewables, the UK electricity supply, transmission, and distribution system need to grow, as clean electricity replaces fossil fuels for industry, heating, and transport. This increases investment requirements that need to sustain the test of geopolitical pressures and places additional stress on land use. Moreover, as renewables get added to the system, electricity markets need to be redesigned to simultaneously manage increased intermittency and deliver the benefits of low-cost renewable energy to consumers. With the reform of electricity market arrangements, the debate on affordability of electricity is at the forefront of policy agendas.

Moving forward with these pillars requires cross-cutting and continued two-way communication and collaboration between academia and policy. Not only is academic evidence critical to optimising policy, but an understanding of policy priorities and real-world challenges can help academics to streamline their research priorities and enable interdisciplinarity. Importantly, energy sits at the heart of the economy and society. The changing weather patterns require energy researchers and decision-makers to interact with new areas that conventionally were left out of the scope of energy system research. For example, new priorities might include assessing how extreme heat resilience correlates with a multitude of physical and mental health impacts and evaluating the implications of AI and cybersecurity improvements on effective energy demand management.

Overall, shifting the energy system will require a portfolio of approaches to guarantee resilience in the UK and more broadly in the global energy system, particularly as the complexity of contingent risks rises. Increased interactions between academics and policy professionals will help build more responsive and flexible policy systems in the UK and bolster its risk preparedness by balancing scientific evidence with the recognition of various policy synergies and trade-offs.

Energy demand

Reducing energy demand is critical for delivering the UK's climate, energy security, and affordability objectives. For that, energy demand must be placed front and centre in UK energy policy.

The frequency and intensity of summer heat waves is intensifying, posing new challenges for the UK's energy demand system. The UK ranks among the top three countries globally in terms of the relative difference in heat exposure between 1.5°C and 2°C warming scenarios. Around 20% of the building stock in the UK is at substantial risk of overheating due to poor ventilation or glazing. Without a more effective adaptation policy, heat-related risks in the UK could triple by 2050, increasing mortality and morbidity rates, reducing labour productivity, creating new pressures on energy, transport, and water infrastructure, and further compounding other environmental stressors.

Heating and cooling could be addressed as interconnected elements of a socio-technical energy system designed to deliver year-round thermal comfort. Increasing frequency and intensity of extreme heat events will add new load to the energy demand system from cooling, and it is important to ensure that it is met without further increasing greenhouse gas emissions. As one of the founding signatories of the Global Cooling Pledge, the UK has already demonstrated global leadership in action for sustainable cooling; leadership which would be deepened by raising its ambition to achieve net-zero cooling emissions by 2050. Delivering this goal will require passive cooling retrofits, minimum efficiency standards for existing homes, and financing instruments such as green mortgages. An integrated energy demand reduction strategy will be key for building multi-level resilience.

Decarbonising the built environment is central to energy demand reduction, and novel approaches are needed to drive this shift. Sustainable solutions for the built environment have robust co-benefits, including increased extreme heat resilience, energy security, and reduction of energy system costs and bills for consumers. However, the poor condition of the UK's building stock means that deep retrofits are often costly and complex to implement at scale, while one-size-fits-all low-emissions heating technology rollouts may face uptake barriers and jeopardise equitable outcomes. Effective building decarbonisation policy will require an integrated, place-based policy approach that accounts for the differences in housing stock, local infrastructure, and community needs. Currently, the more popular fabric-first approaches, which prioritise demand reduction by upgrading insulation, airtightness, and thermal bridging, are insufficient on their own. A more comprehensive strategy would include combining fabric-first approaches with understanding-first approaches, where intervention choices are guided by detailed pre-retrofit assessment, occupant behaviour analysis, archetype modelling, and in-use monitoring.

Social barriers can inhibit effective responses to extreme heat risks. Vulnerability to extreme heat is shaped by social factors, including age, income, and race, which influence households' access to critical social support systems, infrastructure, and the ability to respond to emergencies. Increasing social resilience amidst ongoing changes within the UK's energy demand system will require developing adequate heat risk alert and communication systems; strengthening evidence collection on internal temperatures, urban heat island exposure, and social vulnerability to inform decision-making; and supporting local authorities in incorporating thermal comfort into urban planning, including by mainstreaming Heat Resilience Impact Assessments.

Communication remains a major barrier for placing energy demand at the centre of the UK's energy policy to meet its multiple objectives. Lack of clear and actionable communication between researchers and policymakers has limited the attention to energy demand at the national and local policy levels and slowed necessary investments into energy demand reductions in the built environment. A clearer national strategy on energy demand reduction paired with citizen engagement will be critical to unlocking necessary funding and building democratic support for the energy transition.

Areas for future action

- **Raise ambition to achieve net-zero cooling emissions by 2050 through passive retrofits, efficiency standards, and green mortgages**
- **Develop integrated, place-based building decarbonisation policies that reflect differences in housing stock and community needs**
- **Strengthen social resilience with heat alerts, better data, and Heat Resilience Impact Assessments in planning**
- **Set out a clearer national strategy on energy demand reduction with strong citizen engagement**

Energy storage

Massive scaling of energy storage is essential for the UK to meet its Clean Power 2030 goals and ensure long-term energy resilience, with the National Energy System Operator (NESO) estimating that at least 20GW of installed storage capacity will be needed by 2030. A coordinated, national approach to energy storage would be anchored in capacity scaling, technology diversification, critical minerals security, supply chain resilience, and public trust.

The energy storage industry and battery technologies offer considerable economic opportunities for the UK. The current and projected trends of economy-wide electrification indicate that battery storage technologies can expect to benefit from economies of scale. These trends are global in nature. Developing new battery storage and closed-loop recycling technologies would help address current bottlenecks in the industry and offer the UK an edge in the rapidly growing battery industry.

A resilient energy storage strategy requires a portfolio approach, encompassing short-duration (<6 hours), long-duration (6-160 hours) and seasonal (>160 hours) technologies. Seasonal storage – essential for balancing seasonal variability – is a key challenge due to low technological readiness and high capital costs. While pumped hydro remains the primary seasonal solution currently deployed in the UK, research and development of novel, high-risk, high-reward transformational technologies can help the UK diversify available options and increase the UK's geopolitical security.

Meeting the UK's domestic battery storage requirements necessitates overcoming critical raw mineral (CRM) bottlenecks and reducing supply-chain dependence on China. The supply of energy transition minerals is scarce and strongly geographically concentrated – with China a controlling power of much of the processed supply. The Chinese monopoly on critical raw materials for the energy transition has already triggered a global race over critical mineral mining and processing, contributed to raw material price volatility, and created disruptions across energy storage supply chains. However, the CRM supply pressures will not ease until at least 2040. The UK's dependence on China extends to battery manufacturing, further exposing the UK to supply constraints and geopolitical risks. To mitigate this exposure, the UK must not only invest in domestic manufacturing and recycling infrastructure but also – crucially for benefits to be realised in the mid- to long-term – forge R&D, manufacturing and supply chain partnerships with Europe and nations with world-class research capabilities and/or access to CRM outside of Chinese-controlled supply chains. Strategic collaboration with nations such as Japan, Germany, Australia, and those in Latin America will help diversify and strengthen the UK's supply base, reduce vulnerabilities, and ensure resilience in the battery sector.

Alternative battery chemistries present a key strategic opportunity for the UK. Earth-abundant materials – including sodium-based batteries and Li-sulphur batteries – have strategic value, as they offer cost-effective and geopolitically secure alternatives to lithium-ion. Grid storage could justify development of a dedicated energy storage gigafactory by 2030, but further research is needed to assess their demand profile, commercial readiness, and performance across use cases.

Developing a domestic battery recycling industry is essential to reduce reliance on raw mineral imports, lower lifecycle emissions, and capture second-life battery value. Without increasing recycling capacities and capabilities, the UK is likely to maintain long-term dependencies in the battery supply chain. Currently, there are no large-scale recycling operational facilities in the UK, though this sector is developing.

Over the next decade, as the volume EV market shifts away from nickel-manganese-cobalt (NMC) to lithium iron phosphate (LFP) batteries – which do not contain the more valuable metals found in NMC chemistry – the economic case becomes more challenging. The lower intrinsic value of recovered materials from LFP batteries may impact the commercial viability and scalability of recycling operations. More work is needed to assess the economic case for the longer term.

The UK should seize the opportunity to demonstrate battery material stewardship by investing in the research and development of new battery recycling technologies, to improve efficiencies and drive down costs, and incentivising second-life storage battery applications.

Engaging the public and building trust in battery technologies will support UK's energy resilience. While modern battery systems increasingly meet highest safety standards, public perception often lags behind technical realities. The absence of dedicated UK safety regulations for Battery Energy Storage Systems (BESS) can add to the risks and the perception of risks, leading to community resistance and planning delays. This highlights the need for novel community engagement approaches.

Areas for future action

- **Anchor a national approach in scaling capacity, diversifying technologies, securing minerals, and building supply chain resilience**
- **Invest in R&D for transformational storage technologies and alternative chemistries such as sodium and Li-sulphur**
- **Expand domestic manufacturing and recycling, and forge partnerships with trusted nations to reduce dependence on China**
- **Develop a UK battery recycling industry, improve technologies, and assess long-term economic viability**
- **Introduce safety regulations for battery storage systems and strengthen community engagement**

Energy markets

Electricity market design will shape the UK's ability to deliver a flexible, low-carbon energy system. Meeting the Clean Power 2030 goals requires significant growth in both energy storage (from 1.5 GW to 31.7 GW) and consumer-led flexibility (from 2.5 GW to 10–12 GW). Ensuring that markets can support, enable, and fairly distribute the benefits and costs of this transformation will be critical.

Different retail market governance instruments carry significant trade-offs, making the optimal pathway for energy market redesign both contested and uncertain. Existing market arrangements have delivered important outcomes, including a high share of renewables generation and continued private investment in generation and infrastructure. At the same time, emerging challenges – such as managing variability, enabling distributed flexibility, and maintaining affordability – are placing new demands on electricity markets that were originally designed for centralised, dispatchable systems. For instance, while levy-funded policies supported the expansion of renewable energy-based electricity generation and its integration into the grid, they failed to pass on the benefits of lower costs of renewables to consumers. Similarly, while consumer price caps protect affordability, they may constrain energy efficiency, innovation, or voluntary engagement with more dynamic pricing models.

There is no single optimal model for electricity market reform. Different approaches to pricing (e.g. zonal vs. nodal), consumer participation, and cost recovery involve distinct trade-offs – between simplicity and efficiency, investment certainty and affordability, or national coherence and local responsiveness. These trade-offs must be considered **explicitly and transparently**, involving diverse stakeholder groups that include consumers, industry actors, local authorities, and regulators. Advancing research and evidence on flexibility integration, including lessons from international practice; clarifying the objectives of market reform, including how to balance affordability, decarbonisation, system resilience, and investment certainty in the long term; and facilitating a deliberative process with key stakeholders to assess trade-offs across reform options will be key for **reaching a democratic consensus over market reform.**

Areas for future action

- **Advance research on flexibility integration and draw lessons from international practice**
- **Clarify long-term reform objectives, balancing affordability, decarbonisation, resilience, and investment certainty**
- **Facilitate transparent deliberation with diverse stakeholders on reform trade-offs**
- **Expand inclusive retail flexibility through time-of-use tariffs and smart technologies**
- **Update operational and regulatory frameworks so flexible resources can reliably support the grid**

Retail markets will need to evolve to support consumer engagement with flexibility. This includes expanding access to time-of-use tariffs and smart technologies, while ensuring that participation is voluntary and inclusive. Affordability must remain a central goal in the UK's energy flexibility policy, especially for vulnerable consumers who may face barriers to participation or lack access to enabling technologies.

Flexibility also introduces operational and regulatory considerations. Practices and protocols for grid balancing, market access, and control room operations need to be evolved to ensure that flexible resources, such as batteries, electric vehicles, and smart appliances, can reliably contribute under stress conditions, and build public confidence in flexibility and emerging technologies.

Electricity markets are central to the UK's net-zero pathway. Reform would benefit from being approached as a process of structured, inclusive decision-making that balances competing objectives and builds shared confidence in the flexible energy system.

Human Health

Within the past 20 years, infectious disease outbreaks have increased in frequency and severity. This trend is expected to continue due to the increased risk of zoonotic disease spillover, with pathogens crossing over from animals to humans and causing disease, due to increased exposure from intensive livestock farming, hunting, and habitat loss. This is further compounded by climate change and increases in human population density and interconnectivity through travel and trade.

There is, however, no optimal model for predicting how pathogens will evolve and impact human populations. While potential pathogens have been identified at the UK and global level, and various outbreak prediction and forecasting strategies exist, the levels of uncertainty in these lists and risk for unknown future pathogens termed as 'disease X' remains. This makes it difficult for national governments and public health agencies to prepare and know when and how to respond.

Multiple risks also exist for malicious actors to modify pathogens, to cause widespread severe disease, evade immunity from available vaccines or render treatment to be ineffective. Academic research can support identification, assessment, and mitigation of such risks from biological agents. The area of pathogen detection and discernment of modification is rapidly evolving in the academic field. Academia is well positioned to contribute further to UK security in this area, through innovative technological and research approaches, but there is a need to better align this work with national security needs.

The COVID-19 pandemic demonstrated conclusively policymakers' need for real-time, high-quality data, although the optimal delivery was challenging. Governments took varied approaches to the types and timeliness of different measures, reflecting differences in priorities, capacity in assessing and producing evidence, among a myriad of other factors.

Emergencies such as infectious disease outbreaks and pandemics present a unique challenge as policy makers are required to rapidly understand and respond to new and incomplete information in the context of their existing knowledge and make decisions involving value judgements and trade-offs. Critical information may rapidly change but, in emergency situations, the threshold for what evidence is needed to make an adequate and justifiable decision in the face of uncertainty is a central question. How can policymakers be provided with the tools they need to enable them to understand, analyse, and make such judgements in ways that will enable them to feel confident they are able to explain and justify those judgements when needed?

The human health stream brought together academics and officials from across government departments, public sector research establishments, and research funders to discuss three specific challenges: infectious disease emergence, mitigating risks from deliberate release of biological agents, and decision-making in emergencies. Each challenge discussion was introduced and co-facilitated by different combinations of policy professionals and academics. Key questions for each challenge were presented to the group, prompting a discussion that sought to identify critical issues and explore potential research opportunities for improved biosecurity, and national pandemic preparedness and response.

Infectious disease emergence

Speakers presented an overview of how most emerging infectious diseases are zoonotic in origin and that other factors such as climate change and the increased interaction between humans and animals further increase the risk for spillover.

Key questions for discussion were on how to best coordinate interdisciplinary expertise on infectious diseases, how to make decisions based on risk assessments and on prioritising research investment, and how to best coordinate response and research on human and animal infectious disease emergence and spillover.

Presenters began the session by summarising the new UK Health and Care Research Development Framework for Pandemic Prevention, Preparedness and Response, and then discussing the various research challenges in emerging infections.

The group raised the possibility of evaluating the effectiveness of prioritisation of pathogens in infectious disease outbreak preparedness and response. Participants discussed that pathogen prioritisation may not always be highly predictive. The group considered potential improvements to prioritisation and looking at cross-cutting or pathogen agnostic preparation efforts.

Policy professionals and academics jointly acknowledged the complexity in predicting infectious disease emergence, and that a One Health approach that considers the human-animal interface and the environment, is needed to better understand the drivers of emerging infectious diseases. The group recognised that different sectors need to come together not just during a crisis, but prior to the occurrence of outbreaks or disease spillover.

The group continued to observe that different sectors can work well together in a crisis, but that there need to be more opportunities for various sectors to collaborate in preparing for and practicing outbreak response. Rehearsing and exercising the response to outbreaks with the use of scenario planning may help facilitate collaboration.

Some participants commented that zoonotic threats are likely to emerge outside the UK, which may allow for some time to prepare response plans, but cautioned that data needed to assess and respond may be difficult to access or be unavailable.

Key challenges identified included challenges with regulatory pathways for medical countermeasures such as diagnostics, a mismatch between what academics can provide and what policy makers need.

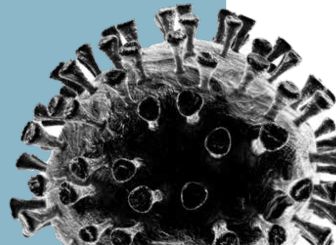
New technologies, such as novel diagnostics, may provide improvements in the speed of the identification of new threats. Some in the group suggested that improvements in diagnostic platforms through speed or being pathogen agnostic may be able to aid in better outbreak response. The group also noted that there is much data available and the need to make better use of it.

Key messages

- Determining and predicting infectious disease emergence is complex and requires transdisciplinary expertise, diverse types of research methodologies and full utilisation of available information.
- The One Health approach is important, and academic-policy collaboration should be done in preparing for outbreaks through scenario planning and testing of existing protocols.
- It's important to integrate colleagues from the Humanities and Arts in preparedness and response efforts. Including and embedding a wide range of disciplines in research programmes would be beneficial.

Areas for future action

- Develop a more inclusive definition for social and behavioural sciences that includes the wider humanities.
- Improve the sharing of information between academics and policy professionals.
- Create more opportunities for different sectors and disciplines to come together and collaborate.
- Evaluate the use of pathogen prioritisation in predicting outbreaks to better understand how to make the approach more effective.
- Work with regulators to speed up or streamline regulatory approval for medical countermeasures such as diagnostics.



Mitigating risks from deliberate biological agents

Stream leads opened the discussion by bringing up the following key questions: How can academics contribute to UK biosecurity through their research agenda and policies? What existing and emerging technologies and academic expertise is available to detect, characterise and respond to a deliberate release scenario and what should be prioritised? What is the role of surveillance systems (wastewater, serologic studies, passive surveillance) in detecting biosecurity events?

Speakers explored the UK Biological Security Strategy, with its mission to implement a UK-wide approach to biosecurity which strengthens deterrence and resilience, projects global leadership, and exploits opportunities for UK prosperity and S&T advantage. Speakers shared examples, such as the work of the Microbial Forensic Consortium, in contributing to UK preparedness against biological risks. They also asked how academia might better inform biosecurity policy priorities, and sparked consideration as to how research could best inform interventions and suitable use of medical countermeasures such as diagnostics.

Many participants emphasised the need to bridge the gap between academic expertise and government policymaking. This includes improving data sharing mechanisms, collaborative platforms, and processes for faster knowledge mobilisation.

Some participants highlighted the abundance of expertise and capability of the UK for biosecurity and on the continued need to build up mechanisms, processes, and direct capacity in new ways. It was emphasised that new and sustained means of collaboration, specifically including industry professionals such as regulators is a major step moving forward.

Participants discussed how academics are often unable to access intelligence and other classified information and suggested that those with expertise on specific pathogens may secure clearance to work with government, and policy makers may provide modified information to researchers that will enable them to assist.

Areas for future action

- To have a process to match the right people with the right expertise and have the right information whilst protecting national security.
- Academics could develop various scenarios and/or previous events to support 'stress testing' response plans.
- To continue improving mechanisms that build a community of practice and advisory pathways that are not just transactional and have clear terms of engagement.
- Reinforce data sharing mechanisms, collaborative platforms, and processes for faster knowledge mobilisation.

The need to develop banks of scenarios and archival records of previous events to improve preparedness and response was also discussed.

Some participants looked at specific approaches, specifically the opportunities and challenges of wastewater surveillance, noting while it has high potential for use with multiple applications in various fields, it is challenging to develop, and systems need to be integrated i.e., sample sharing, longitudinal testing, specimen banking, before establishing a UK-wide programme.

Participants discussed the importance of understanding the source of an outbreak, although early response actions should not be delayed by uncertainties regarding the origin. It was recognised that early identification of the source and intent will be key to inform public perception and may play a role in reducing misinformation.

Key messages

- The response to an outbreak may be similar regardless of origin, but source attribution is important for prevention strategies, for maintaining public trust, and preventing misinformation.
- Deliberate release may involve novel pathogens or non-classical threat agents and outbreaks may be difficult to detect.
- There is a need to better bridge academia and government or Public Sector Research Establishments (PSREs) in preparedness.

Decision-making in emergencies

Stream leads presented questions for the group to consider: What is the optimal process of engagement between scientific advisors and policy makers in health emergencies? What are the key differences in policy making and providing scientific evidence during emergencies that must be considered? How can we best prepare? Which tools, such as scenario planning, can play a useful role? How can policy makers be enabled to have access to high quality, timely analysis and advice to enable them to make value judgements capable of commanding well-founded public trust and confidence?

Presenters shared the perspectives of policy professionals and academics in decision-making during emergencies. From a policy standpoint, engagement of expertise involves decisions on the type of input needed, which mechanisms to use, and navigating information sensitivities, expected response times, and building trust with external experts. From an academic standpoint, there is a need to be clear on the limitations around insights expertise and what research (such as modelling) can provide to inform decision making during emergencies. Presenters also discussed the obligation to the public and how public interest and concern for health may be prioritised differently compared to other crises.

The group addressed the moral obligation for both policymakers and academics to conduct well-designed research during emergencies, and it is essential that such research pays careful attention to its impacts on socially disadvantaged groups, and equity questions. The participants heard discussions on the importance of openness, imagination, and critical reflection with some research needs being specifically concerned at innovating and improving research, policy, and health system interfaces. Speakers shared that a special focus should be placed on value judgements when interacting with these various interfaces.

The participants discussed how there is a need to be aware of biases in selecting who engages with government, to include dissenting or novel perspectives, and those with relevant expertise in areas such as logistics or regulation. A participant mentioned that expertise is also required for policymakers, so that external expert advice can be equitably commissioned and evaluated.

The group heard how effective communication is needed, and that it is not enough to share data, but to ensure it is clearly communicated with the correct interpretation and appropriate use, while being accessible to the intended audience like policymakers or the public.

Participants discussed challenges such as funding needing to be more responsive during emergencies, the need to build and sustain resilient networks of expertise and having a model that requires or incentivises collaboration. Participants expressed that there are differences in expert advice requirements during a crisis compared to in pandemic "peacetime." Crisis conditions contribute additional pressure on academic time, particularly when academics are accountable to funding requirements and timelines. Participants also discussed that expert advice to shape policy should be funding agnostic.

Key messages

- Reminder of the obligation of policy professionals and academics to communicate and engage with the public during a health emergency response.
- Caution with established connections and the risk of *group think*. People with different views need to be included.
- Including industry experts may provide real-world experience in areas such as logistics, manufacturing, or regulation.
- Data must not only be shared but communicated clearly to ensure correct interpretation and appropriate use.

Areas for future action

- Build networks *before* emergencies.
- Learned societies may help in identifying experts best suited to aid in decision making.
- Determine ways to maintain active decision making and institutional memory during inter-pandemic periods.

Technology

Novel digital innovations continue to shape society in unprecedented ways. They have the potential to not just disrupt our normal ways of life but fundamentally transform the human experience. From artificial intelligence to advanced automation and neurotechnology, our world is becoming deeply technologically integrated and interdependent. We stand on the cusp of an exciting yet challenging new reality and must work together to shape our shared future.

Any new technology brings new opportunities and risks. As technology proliferates, and as our reliance on it deepens, the security of that technology becomes increasingly paramount to the resilience of the societies and systems that rely on it. Nations must therefore prioritise the cybersecurity of emerging technology as a fundamental enabler of future national cohesion, prosperity and security.

Participants in the Technology Stream discuss the cybersecurity risks, opportunities, and solutions of one of the UK's, and the world's, leading digital disruptors: Artificial Intelligence (AI).

Following the explosion of large language models (LLMs), a particular type of AI, into global consciousness in 2022, 2025 marks a pivotal milestone in AI's practical deployment throughout economies. Transformative deployments of LLMs are now documented in areas as diverse as law, coding, creative industries, and healthcare. Through these deployments we have witnessed a demonstratable shift from AI hype to transformational adoption, while the technology continues to rapidly mature and evolve. The question is no longer if AI will change things, but by how much. And consequently, we must ask ourselves not whether we should adapt, but how we can best do so.

From a security perspective, contemporary AI is a technology that brings transformative risks and opportunities at different scales: the technological systems themselves; the ecosystems they are connected to; and the broader global environment they underpin. At each scale, the cybersecurity researchers, practitioners, and policy professionals must not only consider how AI is transforming the nature of risks we face and how these risks might be controlled, but also how it can be leveraged to enhance cybersecurity controls. Not all current risk controls will transfer and be applicable to AI and we can therefore expect transformations in how we control risks.

These cybersecurity risks and opportunities, and their application across the various interconnected scales, are of growing interest to governments, industry, and academia. Only through understanding both the risk and opportunities will we be able to effectively advance digital resilience and unlock the benefits of AI.

However, analysing and advancing AI cybersecurity is a complex process. The pace of AI development and adoption, combined with the centralisation of specialised knowledge and resources within limited organisations leading the advancement of AI in key geographical areas, presents significant challenges to enhancing resilience and unlocking the cybersecurity opportunities of AI. Overcoming these challenges and building a secure AI future requires a multistakeholder and multidisciplinary approach between government, academia, and industry.

Each of these groups hold unique priorities and perspectives related to the topic but struggle to work together to holistically advance AI cybersecurity. Too often they are siloed and lack the time or capacity to connect. This prevents the cross-pollination of ideas and constrains their ability to develop collaborative and effective approaches. The current fragmented approach threatens to not only constrain progress in securing AI as a technology but benefits bad actors seeking to exploit these systems for their advantage.

To bring these stakeholders together and help to address these challenges, the Technology Stream convened a diverse range of experts from each of these stakeholder groups to discuss issues related to three critical topics: cybersecurity of AI, securing AI supply chains, and AI opportunities for cybersecurity. Each of topic represents an essential area for building future resilience for the UK's national AI and broader technology ecosystem and enabling future opportunities. While robust and inclusive in design, these discussions could have been strengthened through greater representation from industry stakeholders, particularly AI developers. Consequently, commentary and feedback from the developer community on this report is welcomed as a means of further advancing and improving the analysis.

The following sections outline a summary of the discussions held across three sessions, as well as key messages and areas for future action. Many of the issues were interrelated, so the sections are best understood as a whole.

Cybersecurity of AI

The cybersecurity of AI systems themselves is a foundational aspect of providing resilient technology, maintaining consumer confidence, and facilitating novel and scaled deployment. Participants discussed the range of human and technical vulnerabilities that AI systems may be exposed to and agreed that some vulnerabilities remain typical of regular digital technologies, while others are unique to AI. Overall, most participants agreed that understanding and addressing these vulnerabilities remains an ongoing challenge.

The UK's Department of Science, Innovation and Technology's (DSIT) Code of Practice for the Cyber Security of AI, the European Telecommunications Standards Institute's (ETSI) Technical Specifications 104 223 and the G7 AI Principles Code of Conduct were discussed as leading guidelines for managing security issues related to AI systems. However, most participants agreed that there is a need to both create consensus around the security controls required to implement these guidelines, and to prepare the cybersecurity industry to support organisations in adopting these controls for their AI systems, before these guidelines can operationally be implemented.

Several Participants linked these challenges to a limited understanding of AI system components themselves. Both developers and adopters of AI systems are generally perceived to lack a comprehensive understanding of the 'ingredients' (e.g., data provenance) used within their systems, and therefore oversight of where vulnerabilities may originate from. This has led to lack of transparency and traceability associated with the technology overall, which has made it difficult for cybersecurity practitioners to implement measures that advance AI system resilience and has spread concerns as to data trustworthiness.

Associated with these challenges, there is also a narrow understanding of which traditional cybersecurity controls are effective on AI systems, and which are not. Discussions highlighted that there is considerable confusion, especially amongst AI adopters, over what novel risks and associated controls AI systems require versus what existing controls may be effectively transferred to these systems. Many participants suggested that this may stem from both the transparency and traceability issues previously mentioned, and a lack of integration between the cybersecurity and AI communities, many of whom operate in silos. Therefore, greater integration between these two communities, and a more robust knowledge of what human and technical risks require existing or novel controls, was presented as a proactive pathway to accelerating the secure enhancement of AI systems.

Finally, at a foundational level, most participants also highlighted a lack of necessary incentives to motivate or mandate the secure design and deployment of AI systems to help reduce the number of vulnerable products being taken to, and utilised in, the market. While it was agreed that commercial companies in competitive markets are driven by first-mover advantage and required to develop their products quickly, it was also agreed that their commercial motivations should be balanced with 'secure by design' principles to help mitigate vulnerabilities early in the product lifecycle. Similarly, while entities may be seeking to rapidly adopt AI to leverage its various benefits, it was agreed that adopters should simultaneously be introducing appropriate cybersecurity controls (where known) to protect their expanded digital attack surface.

Participants did not find agreement on what incentivisation measures should be introduced but suggested that creative use of both positive (carrot) and punitive (stick) measures could be considered to appropriately balance the need for AI innovation and security. When designing incentives, balancing the cost of investing in security (e.g., curating data) and responding to incidents should be considered and brought to the attention of AI developers and adopters.

Areas for future action

- Research could be undertaken to develop a comprehensive and open knowledge base of AI system components, structures and vulnerabilities to help improve transparency, facilitate greater traceability and improve security.
- Work could be undertaken to bring the AI and cybersecurity communities closer together to enable more collaboration and facilitate a greater understanding of the nature of evolving risks in the AI domain.
- Efforts could be undertaken to develop a consensus on necessary and effective cybersecurity controls for AI (technical and administrative). This could include identifying and sharing what existing cybersecurity controls may be effectively applied to AI, and what new risks require new controls.
- Measures could be taken to boost industry preparedness to provide necessary and effective novel controls to organisations adopting AI.
- Action could be taken to identify and implement incentives that guide the adoption of secure AI cybersecurity practices. Consideration should be given to how to effectively balance and incentivise measures.

Securing AI supply chains

Technological supply chains are an area of increasing threat activity and geopolitical complexity. Cybersecurity incidents proliferate through supply chains, with their consequences affecting entities up- and downstream from the original impact point. Given contemporary market structures, these risks are likely to extend beyond sectors and national boundaries. Therefore, AI cybersecurity considerations must include both national and international supply-chain perspectives to develop comprehensive AI ecosystem resilience.

As in Session 1, some participants highlighted DSIT's Code of Practice for the Cyber Security of AI and the European Telecommunications Standards Institute's (ETSI) Technical Specifications 104 223 as leading examples for managing AI supply chain cybersecurity. However, again, it was suggested by some participants that while these resources provide a foundation for managing AI supply-chain security, more detailed supplementary guidance is required to secure AI supply-chain risks in practice. Furthermore, it was noted that targeted guidance is needed for both the *providers* and *adopters* of AI, who may consider different factors based on their market and supply chain contexts. General guidance that does not address the nuanced cybersecurity differences between these two groups will not equip stakeholders to effectively manage their risk environment.

Nevertheless, despite their contextual differences, several cross-cutting challenges were identified for both providers and adopters of AI. These include an underdeveloped taxonomy of AI supply chain components and risks, and a limited understanding of how risks may propagate up- and downstream of cyber incidents. Currently, a lack of consensus on the factors and risk within the scope of AI supply chain cybersecurity is undermining efforts to develop greater resilience at the organisational, national and international levels. While these challenges are not necessarily unique to AI and exist more widely in cyber supply-chain management, most participants agreed that they are all currently affecting AI cyber supply-chain management and require specific attention.

Concentrated market dynamics was another cross-cutting risk identified for both providers and adopters of AI. In several key supply-chain areas including hardware, cloud computing and skills, a few large and highly specialised entities dominate the market. While it was recognised that this concentration may provide efficiency dividends, participants agreed that a lack of market diversity also brings single-point-of-failure and sovereign-capability risks.

More generally the issue of incentivising cybersecurity controls was discussed in the context of globalised supply chains where there are reported difficulties implementing either effective positive or punitive incentives. In addition to obvious cross-border jurisdictional challenges, discussions also linked the issue of incentivisation to the wider taxonomy, transparency and AI system vulnerability challenges outlined above. Each of these challenges create difficulties in understanding and scoping both the risks and solutions and consequently exacerbate the complexities of cyber supply-chain management.

For example, when considering procurement requirements for enforcing upstream adoption of secure design and development principles, some participants expressed concern that it would be difficult to introduce effective requirements if the components of these requirements are not mutually understood, if AI systems' 'ingredients' are opaque, or if the vulnerability of those systems remains unknown. Therefore, it was suggested that an holistic approach to analysing AI cyber supply chains that includes considerations of both definitional and incentivisation challenges, in addition to detailed technical guidance, would be best suited to identifying and managing risks.

Areas for future action

- Collaborative efforts could be pursued to develop a consensus- driven taxonomy of the AI cyber supply chain between different stakeholder groups across the AI cyber ecosystem.
- Building on the Software Bill of Materials (SBOM), efforts could be made to develop an AI Bill of Materials (AI BOM) to identify the 'ingredients' of the AI cyber supply chain and increase the transparency and traceability of AI systems.
- Action could be taken to map AI system vulnerabilities at an ecosystem level to help better understand AI supply chain risks, how these risks propagate, and which controls are effective.
- Work could be undertaken to identify and implement ecosystem level AI cybersecurity incentives that guide the adoption of cyber secure practices throughout the AI supply chain. This work should be aligned to and build on local or domestical level incentivisation efforts discussed in the section above.
- Efforts could be undertaken to identify AI market concentration risks and develop mitigation strategies. This work should include considerations for how these factors may introduce broader ecosystem and sovereignty risks.

AI opportunities for cybersecurity

AI presents transformative opportunities in the cybersecurity domain by reducing bottlenecks and increasing the efficiency and effectiveness of cybersecurity operations. These opportunities may include autonomous defences, advanced information-sharing, or improved physical infrastructure protections. AI may also enable technological 'leapfrogging' to rapidly advance security and could offer solutions to human-centred cybersecurity problems. To capitalise on these opportunities, however, many participants suggested that it is essential to be bold and creative when approaching AI and not think of the technology as 'just another security widget.' If a bold approach is not adopted, then it was suggested by most participant that there is a risk the defensive benefits of AI will be outpaced by the offensive benefits it offers to adversaries.

Beyond simply being bold and receptive to transformative change, discussions also highlighted several structural barriers to unlocking AI's cybersecurity opportunities. These include: a shortage of skilled workers to grow the market; infrastructure and resource limitations (i.e., limited data centre, power and water supply); consumer uncertainties surrounding AI's cybersecurity capabilities and uses; restricted international interoperability; and slow governance frameworks. To overcome these barriers, a 'triple helix' approach to public private partnerships (PPPs) that involves government, academia and industry was identified by some participants as a mechanism for building trust, aligning key stakeholder communities, understanding challenges and facilitating collaborative problem solving. Inclusive PPPs that incorporate SMEs and large enterprises were suggested by some participants as a potential means for developing a growth-enabling marketplace that supports businesses to innovate and scale AI opportunities for cybersecurity.

Greater research into and transparency around the application of AI for cybersecurity purposes was agreed as a means for improving explainability, building trust in AI cybersecurity solutions and overcoming consumer uncertainties. Currently, there is a perception that the cybersecurity industry has not provided robust and consistent AI cybersecurity use-cases, and that this is undermining user trust and uptake of potential solutions, as well as further innovation and growth in the AI cybersecurity domain. To overcome this challenge, applications of AI for enhanced cybersecurity should be widely and transparently documented by industry and academia in clearly communicable use cases that boost consumer confidence.

Finally, to address issues surrounding international operability, attendees highlighted engaging with international partners and processes to advance cohesive global AI governance as a necessary component for enabling AI cybersecurity innovation and adoption. Through building a simplified and complementary global AI environment, businesses will be provided with greater certainty to develop scalable security solutions and be empowered to capitalise on AI cybersecurity opportunities.

Areas for future action

- Strategic investments could be made into addressing structural barriers to unlocking AI's cybersecurity opportunities, including in areas of skills development and enabling infrastructure.
- PPPs could be considered as potential mechanisms for bringing stakeholder groups together and identifying and addressing various barriers to AI cybersecurity innovation and market growth.
- Efforts could be undertaken to document and communicate the effective use of AI for enhanced cybersecurity to build consumer confidence and facilitate opportunities.
- Action could be taken to develop a cohesive and efficient AI governance environment that advances cross-market synergies, introduces greater certainty, and encourages innovation and growth in the application of AI for cybersecurity.

Further reading

Energy & Environment

Barrett J, Pye S, Betts-Davies S, et al. Energy demand reduction options for meeting national zero-emission targets in the United Kingdom. Nature Energy. 2022;7:726–735. doi:10.1038/s41560-022-01057-y

Mihalache AE, Hampton S, Darby S. Domesticating energy flexibility: Learning from Great Britain's 2022–2023 demand flexibility service. Energy Efficiency. 2024;17:88. doi:10.1007/s12053-024-10268-z

Rosenow J. Beyond supply: The case for decarbonising energy demand. PLOS Clim. 2025;4(3):e0000590. doi:10.1371/journal.pclm.0000590

Sahakian M, Fawcett T, Darby S. Energy sufficiency in buildings and cities: current research, future directions. Buildings and Cities. 2024;5(1):692–703. doi:10.5334/bc.519

Whitmarsh L, Hampton S. Are radical changes to lifestyles necessary for mitigating climate change? Dialogues on Climate Change. 2024;1(1):23–29. doi:10.1177/29768659241293215

Faraday Institution. Insight 11: Sodium-ion Batteries – Inexpensive and Sustainable Energy Storage. By Scott Lilley. May 2021. Available from: https://www.faraday.ac.uk/wp-content/uploads/2021/06/Faraday_Insights_11_FINAL.pdf

Faraday Institution. Insight 20: Developing a UK Lithium-ion Battery Recycling Industry. By Jonathan Leong. July 2024. Available from: https://www.faraday.ac.uk/wp-content/uploads/2024/07/Faraday_Insights_20_FINAL.pdf

Faraday Institution. Insight 21: Batteries in Stationary Energy Storage Applications. By John-Joseph Marie. October 2024. Available from: https://www.faraday.ac.uk/insights/insight-21-batteries-in-stationary-energy-storage-applications/

Harper GDJ, Kendrick E, Anderson PA, Mrozik W, Christensen P, Lambert S, et al. Roadmap for a sustainable circular economy in lithium-ion and future battery technologies. J Phys Energy. 2023;5(2):021501. Available from: https://eprints.lse.ac.uk/118420/1/Harper_2023_J._Phys._Energy_5_021501.pdf

Innovate UK, Warwick Manufacturing Group, The University of Warwick. Sector-wide UK Battery Demand Projections to 2035. 25 Apr 2025. Available from: https://www.ukri.org/publications/cross-sector-battery-report/

Rho Motion, Faraday Institution. Market and Technology Assessment of Grid-Scale Energy Storage Required to Deliver Net Zero and the Implications for Battery Research in the UK. Sept 2023. Available from: https://www.faraday.ac.uk/wp-content/uploads/2023/09/20230908_Rho_Motion_Faraday_Institution_UK_BESS_Report_Final.pdf

Royal Society. Large-scale Electricity Storage. Sept 2023. ISBN: 978-1-78252-666-7. Available from: https://royalsociety.org/-/media/policy/projects/large-scale-electricity-storage/large-scale-electricity-storage-report.pdf

Human Health

R&D Blueprint, World Health Organization. Pathogens prioritization: a scientific framework for epidemic and pandemic research preparedness. Geneva: World Health Organization; 2024. Available from: https://www.who.int/publications/m/item/pathogens-prioritization-a-scientific-framework-for-epidemic-and-pandemic-research-preparedness

UK Health Security Agency. Priority pathogen families research and development (R&D) tool. London: Department of Health and Social Care; 2025.

Musunuri S, Sandbrink JB, Monrad JT, Palmer MJ, Koblentz GD. Rapid proliferation of pandemic research: implications for dual-use risks. mBio. 2021;12(5):e01864-21. doi:10.1128/mbio.01864-21

Managing risks of research misuse: joint policy statement [Internet]. London: UK Research and Innovation; 2016. Available from: https://www.ukri.org/publications/managing-risks-of-research-misuse-joint-policy-statement/

Blavatnik School of Government. COVID-19 Government Response Tracker [Internet]. Oxford: University of Oxford; 2020. Available from: http://www.bsg.ox.ac.uk/research/covid-19-government-response-tracker

Paparella G, Elahi S, Hoffman SJ, Shindo N, Alobo M, Norton AJ, et al. Medical and social scientists as strategic advisors: The case of GloPID-R in 2021. Calif Manag Rev Insights [Internet]. 2023 May 1. Available from: https://cmr.berkeley.edu/2023/05/medical-and-social-scientists-as-strategic-advisors-the-case-of-glopid-r-in-2021/

Technology

World Economic Forum. Artificial Intelligence and Cybersecurity: Balancing Risk and Rewards. Industries in the Intelligent Age White Paper Series. Geneva: World Economic Forum; 2025. Available from: https://www.weforum.org/publications/industries-in-the-intelligent-age-white-paper-series/cybersecurity/

UK Government (Department for Science, Innovation & Technology). The AI Cyber Security Code of Practice. London: DSIT; 2025. Available from: https://www.gov.uk/government/publications/ai-cyber-security-code-of-practice

European Telecommunications Standards Institute (ETSI). TS 104 223 – Securing Artificial Intelligence (SAI): Baseline Cyber Security Requirements for AI Models and Systems. Sophia Antipolis: ETSI; 2025. Available from: https://www.etsi.org/deliver/etsi_ts/104200_104299/104223/01.01.01_60/ts_104223v010101p.pdf

G7. Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems. 2023. Available from: https://www.mofa.go.jp/files/100573473.pdf

Acknowledgements

Funders
Blavatnik School of Government
Research England (Policy Support Fund)
ZERO Institute

Partners
Blavatnik School of Government
Oxford Martin School
Pandemic Sciences Institute
Policy Engagement Team
ZERO Institute

Selected participants
Adam Moore, Deputy Head of the Chemical, Biological and Radiological Security Taskforce, Cabinet Office
Adam Suttle, Portfolio Manager, Energy & Decarbonisation Team, Engineering and Physical Sciences Research Council
Alessandra Lo Fiego, Scientific Programme and Collaboration Manager, University of Oxford
Alexander Betts, Pro-Vice Chancellor for External Engagement, Sport, and Community, University of Oxford
Alice Norton, Associate Professor, University of Oxford
Alisa Ghura, Energy Analyst, Hygen Energy
Amanda Rojek, Clinician Researcher, University of Oxford
Anca-Elena Mihalache, Head of Smart Energy Policy, Department for Energy Security and Net Zero
André Neto-Bradley, Lead Energy Research Advisor, Department for Energy Security and Net Zero
Andrew Bell, Energy Resilience, Department for Energy Security and Net Zero
Ben Noone, Wholesale Market Strategy Lead, National Energy System Operator
Beatrix Coppack, Crisis Response and Preparedness Team Leader, Department for Environment, Food and Rural Affairs
Çağatay Yücel, Senior Research Associate, University of Oxford
Carmen Galán-Marin, Professor, Universidad de Sevilla
Carolin Weisser Harris, Lead International Operations and Technical Board Member, University of Oxford
Charles Godfray, Professor of Population Biology, University of Oxford
Charlotte Hall, Head of Health Protection Research, Department of Health and Social Care
Daniel Reumann, Postdoctoral Research Associate, University of Oxford
Darren Lewis, Senior Lead, Plexal
David De Roure, Professor of E-Research, University of Oxford
David Howey, Professor of Engineering Science, University of Oxford
David Pyle, Professor of Earth Sciences, University of Oxford
Deirdre Hollingsworth, Professor of Infectious Disease Epidemiology, University of Oxford
Edward Venmore-Rowland, Head of AI Cybersecurity Policy, Department for Science, Innovation and Technology
Emily Adams, Associate Professor, University of Oxford
Gustė Gurcinaite, Doctoral Student, University of Oxford
George Bowman, Deputy Director, Cabinet Office
Gesche Huebner, Professor of Environment and Human Health, University of Exeter
Gian Melloni, Programme Manager, University of Oxford
Graeme Clark, Defence Science and Technology Laboratory
Hannah Peel, Team Leader, National Security and Resilience Team, Government Office for Science
Harry Parker, Team Leader, Energy Security Strategy Coordination, Department for Energy Security and Net Zero
Harry Scoble, Programme Manager, Fortescue Zero
Hester Kan, Programme Coordinator, University of Oxford
Helena Dodd, Governance and Risk Lead, Foreign, Commonwealth & Development Office
Holly Sadler, Research and Policy Advisor, University of Oxford
Ingrid Aguiar Schlindwein, Research Associate, University of Oxford
Ioannis Agrafiotis, Senior Cybersecurity Researcher, University of Oxford
Jack Umenberger, Senior Research Fellow, University of Oxford
Jaqueline Broadhead, Director of the Global Exchange on Migration and Diversity, University of Oxford
James Leeke, Director Programme Delivery, Plexal
James Pride, Policy Lead, Climate Adaptation, Department for Energy Security and Net Zero
Jamie Saunders, Strategic Security Consultant, University of Oxford
Jan Rosenow, Jackson Senior Research Fellow, University of Oxford
Jassim Happa, Senior Lecturer, Royal Holloway University of London
Jake Dunning, Senior Researcher, University of Oxford
Joe Fulwood, Global Engagement and Communications Officer, University of Oxford
Jonny Buzzing, Energy Consultant, LCP Delta
Julia Dickinson, PSI Research Strategy, Delivery and Cultural Lead, University of Oxford
Julia Morse, Associate Professor of Political Science, University of Santa Barbara
Katrina Lythgoe, Professor of Infectious Disease, University of Oxford
Karen Meadows, Deputy Chief of Staff and Head of Office, Home Office
Mark Harrison, Professor of the History of Medicine, University of Oxford
Mark Saunders, Energy Systems and Investments Manager, Oxfordshire County Council
Marialena Nikolopoulou, Professor of Sustainable Architecture, University of Kent
Mary De Silva, Deputy Chief Scientific Advisor, Department of Health and Social Care
Matthew Howard, Chief Strategy Officer, The Faraday Institution
Mel Cowans, Visiting Researcher, University of Cambridge
Melanie Garson, Associate Professor, University College London
Melissa Hamilton, Professor of Law and Criminal Justice, University of Surrey
Michael Parker, Professor of Bioethics, University of Oxford
Ngaire Woods, Professor of Global Economic Governance, University of Oxford
Nick Eyre, Emeritus Professor of Energy and Climate Policy, University of Oxford
Nick Joicey, Chief Operations Officer, University of Oxford
Obaid Ashraf Shah, Principal Sustainability Specialist, Department for Transport
Paolo Cerrado, Research Assistant, University of Oxford
Patricia Esteve-Gonzalez, Research Fellow, University of Oxford

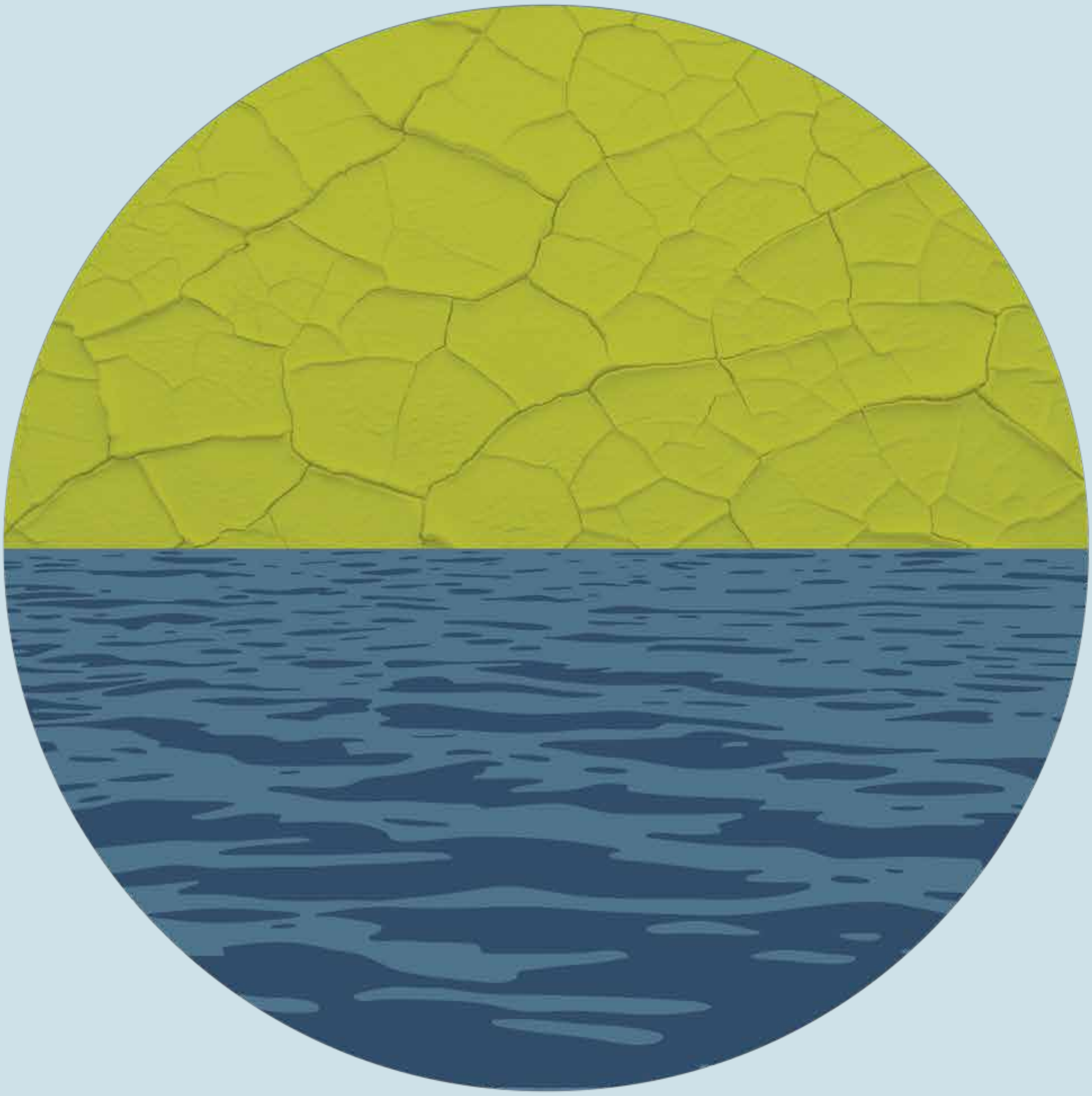
Paul Miller, Deputy Director of CSIT, Queen's University Belfast
Paul Shearing, Professor of Sustainable Energy Engineering, University of Oxford
Peter Horby, Professor of Emerging Infections and Global Health, University of Oxford
Pippa Vanderplank, Principal Researcher, Department for Energy Security and Net Zero
Radhika Khosla, Associate Professor, University of Oxford
Representative from National Cyber Security Centre
Rex Amos, Head of Strategy, Laboratory for AI Security Research, Foreign, Commonwealth & Development Office
Roger Hargreaves, Director, Cabinet Office
Rodrigo Furst, Postdoctoral Research Scientist, University of Oxford
Roxana Radu, Associate Professor of Digital Technologies and Public Policy, University of Oxford
Rose Dickinson, Carbon Reduction Team Manager, Oxford City Council
Sadie Creese, Professor of Cybersecurity, University of Oxford
Sassy Molyneux, Professor of Global Health, University of Oxford
Shreyasi Kudpi Rao, Policy Analyst, Utility Warehouse
Stephen Ingarfield, REMA, Department for Energy Security and Net Zero
Stephen Roberts, Professor, University of Oxford
Steve Oakeshott, Head of Infections and Immunity, UK Research and Innovation
Tina Fawcett, Associate Professor, University of Oxford
Toby Bonvoisin, Doctoral Student, University of Oxford
Tom Jeffery, Co-Director of Defence and National Security, Alan Turing Institute
Tom Sutton, Government Office for Science
Vikaran Khanna, Technology Insights Lead, National Energy System Operator

Event management team
Anna Dominey
Aileen Marshall-Brown
Charlotte Medland
Jessica Hedge
John Styles
José Rojas Alvarado
Juliette Scott-Barrett
Naomi Gibson
Noora Kanfash
Rebecca Jones
Rosaleen Cunningham
Umme Hani Imani
William Pryor

Photographer
Stuart Gillespie

Email: researchandpolicy@admin.ox.ac.uk | **Website:** https://www.ox.ac.uk/open

LinkedIn: www.linkedin.com/company/oxford-policy-engagement-network | **Bluesky:** @oxpolicyengaged.bsky.social



UNIVERSITY OF OXFORD

OPEN OXFORD POLICY ENGAGEMENT NETWORK

BLAVATNIK SCHOOL OF GOVERNMENT

ZERO INSTITUTE

PANDEMIC SCIENCES INSTITUTE

OXFORD MARTIN SCHOOL