Security and resilience of energy infrastructure: an enquiry from the Parliamentary Office of Science and Technology (POST)

About the IET

The IET is a trusted adviser of independent, impartial, evidence-based engineering and technology expertise. We are a registered charity and one of the world's leading professional societies for the engineering and technology community with over 156,000 members worldwide in 147 countries. Our strength is in working collaboratively with government, industry, and academia to engineer solutions for our greatest societal challenges. We believe that professional guidance, especially in highly technological areas, is critical to good policy making.

Executive Summary

Developing resilient and secure energy infrastructure is essential to supporting the UK's economic growth, public services and Net Zero ambitions. As the country transitions towards Net Zero, significant changes to energy generation, distribution and consumption patterns will be required and in many instances are often already underway. Consequently, new risks and vulnerabilities are emerging across both physical and digital infrastructure. To manage these challenges, government and industry must adopt a whole-system approach to resilience, recognising the interdependencies between energy networks, operational technologies, supply chains and wider critical national infrastructure. Embedding resilience and security into infrastructure planning from the outset will help ensure that the transition to a low-carbon energy system remains reliable, adaptable and secure.

The Clean Power 2030 Action Plan presents significant capacity targets for implementation of batteries and long-duration storage, interconnectors and consumer-led flexibility as well as renewables. With low carbon dispatchable power also considered alongside other potential sources such as gas carbon capture, utilisation, and storage (CCUS) and hydrogen-to-power (H2P).

Digital technologies, as part of a holistic whole systems approach, will have a vital role to play in strengthening resilience. Enhanced monitoring, data analytics, artificial intelligence (AI) and digital twins can improve operational visibility, support scenario modelling and enable better-informed decision-making. However, greater digitalisation also increases exposure to cyber threats. The energy sector is an increasingly attractive target for cyber criminals and hostile state actors, therefore, robust cyber security measures, incident response planning and workforce capability are critical components of national resilience.

Alongside a whole-system engineering approach, developing cyber expertise, strengthening security cultures, and regular test response and recovery plans against recognised standards, will be key to creating a resilient energy infrastructure. This is essential to ensuring that infrastructure remains reliable, adaptable and secure throughout the transition.

Together with cyber resilience, the UK must continue to strengthen the physical security of critical energy assets, particularly in the North Sea, where offshore wind infrastructure, subsea cables, telecommunications networks and gas pipelines form a vital part of the nation's energy system. There have been several high-profile incidents in recent years that have demonstrated that attacks on critical infrastructure are a credible threat, requiring greater investment in asset protection, monitoring technologies and international cooperation. By combining investment in resilience, cyber security, digital innovation and skills development, the UK can build a secure and resilient energy system capable of supporting energy security, economic prosperity and the successful delivery of Net Zero.

Recommendations

- **Response plans:** Stronger requirements for cyber security response plans. Cyber security is not just about prevention, but businesses should model their response in the event of a breach to identify weaknesses as a part of routine response planning. Further cyber security and resilience recommendations can be found in our position paper.
- **Energy resilience:** As the UK energy system becomes increasingly dependent on renewable generation, interconnection and power-electronics-based infrastructure, electricity system resilience, effective asset management, and security of supply becomes more important.
- **Effective management:** There needs to be appropriate and proactive management of critical assets, investment in network resilience, and enhanced protection of energy infrastructure to reduce the risk and impact of failures, outages and other disruptions.

Cyber security and building resilience through digital

The energy sector's increasing reliance on digital systems has made it a prime target for cyber-attacks and the consequences of a successful attack can be devastating. Cyber security is a critical part of ensuring the safety and resilience of the UK's energy infrastructure. In 2023, 90% of the world's largest energy companies suffered cyber security breaches, with critical infrastructure increasingly becoming a primary target for state-sponsored hackers and cybercriminals (Growing cyber security threats in the energy sector and how businesses stay resilient, RenewableUK, 2025). The cost of these breaches is also potentially crippling for companies, with cyber-attacks costing UK businesses an estimated £64 billion annually, with £37.3 billion in direct costs and £26.7 billion in indirect costs (The True Cost of Cyber Attacks: Balancing business protection and risk, ESET, 2025). As cyber security threats are continually evolving, the government should ensure businesses are supported by qualified cyber security experts and accredited professional bodies.

Despite the risks that digital systems may pose to security, digital technologies can help bolster resilience across the energy infrastructure by providing a greater insight into scenario modelling and provide insightful data analytics to help inform decision making. However, as with any other technology, it can also pose its own risks, and it is important to be aware of vulnerabilities that digital technologies may introduce to a system of systems.

Energy infrastructure outages can have widespread and serious consequences for both individuals and society and the repercussions of energy infrastructure failing due to AI misinformation or cyber security can be significant. The increase in the number of devices

connected by digital networks exposes the grid to new risks and misinformation can be a tool of cyber attackers aiming to disrupt grid operations. AI-driven malicious misinformation campaigns could mislead operators or automated systems, causing disruptions and outages, while AI systems manipulated by false data may also introduce vulnerabilities that hackers can exploit, leading to misleading analyses, faulty decision-making, and increased security risks. In order to minimise this risk, it is imperative to develop a better, broader definition of safety and risks of AI tools, this will also help AI developers ensure their product is safe and fit for purpose before going to market. This will lead to robust and transparent AI systems that are subject to comprehensive ongoing validation and verification processes (Spending Review 2025, IET, 2025). There should also be effective cyber security measures to protect AI systems from manipulation. Communicating the potential threats and risks around AI will increase awareness, develop competence, and create the correct cyber security culture within an organisation. This will make the UK a leader in AI safety.

Reskilling and upskilling are critical to ensuring robust cyber resilience on a day-to-day basis. A cyber cultural change needs to be encouraged through greater learning and cyber awareness, to ensure that the UK is protected from the increasing threat of cyber-attacks. According to the latest IET Skills Survey one of the most important digital skills that employers ranked highly for growth is cyber security (38%), however cyber security is also the digital skill that employers find the most difficult to recruit for (17%) (UK Engineering and Technology skills survey, IET, 2025).

The use of digital twins, supported by a combination of technologies, can also help support greater resilience across energy infrastructure. A digital twin is a "virtual model of an object, a system, or a process. It is connected to its real-world counterpart by a 2-way flow of right-time data, meaning it mimics it in all aspects." (What a digital twin is and how you can contribute, GOV.UK, 2024). They are widely used across different sectors to test decisions before they are made and understand how different actions might affect the real world. Digital twins can predict and model scenarios to help build resilience into national and energy infrastructure, however, there is often a lack of clarity about what a digital twin is with products being mislabelled as such. It is important to ensure clear labelling and expertise to ensure that it is fit for purpose and a good use of investment.

A priority for digital twin and smart grid development may be the challenge of optimising a future energy system characterised by increasing complexity. This includes integrating variable renewable generation with differing output profiles (such as wind and solar), alongside energy storage, interconnection, and dispatchable low-carbon generation. It also requires managing growing electrification of transport and heat, while harnessing demand-side flexibility to balance the system efficiently. Focusing digital twin capabilities on these whole-system integration challenges is likely to deliver greater value than narrower applications.

Energy infrastructure

Sabotaging key UK energy infrastructure is a growing national security and energy resilience concern with recent discussions within Parliament and national security circles have highlighted growing concerns regarding the vulnerability of modern democracies to digital threats (Cyber Security and Resilience (Network and Information Systems) Bill, House of

Lords, 2026). The importance of electricity system resilience, effective asset management, and security of supply therefore increases as the UK energy system becomes further dependent on renewable generation, interconnection and power-electronics-based infrastructure. There needs to be proactive management of critical assets, investment in network resilience, and enhanced protection of energy infrastructure to reduce the risk and impact of failures, outages and other disruptions.

North Sea

The North Sea contains a dense network of essential infrastructure, including gas and oil pipelines, electricity transmission cables, offshore wind assets and telecommunications links, making it strategically important to the UK's energy system. Evidence from the North Sea Transition Authority (NSTA) 2024 report indicates that remaining UK gas resources are estimated to range between 4,627 TWh and 11,288 TWh with a central estimate of 7,589 TWh (Gas system in transition: Security of supply, IET, 2026). At current rates of production, this would equate to approximately 20 years of supply. As such, the UK should work with neighbouring countries to protect pipelines as well as other essential offshore infrastructure. In April 2024 between the UK, Norway, Germany, Denmark, Belgium and the Netherlands, it was agreed to improve cooperation on protecting critical subsea energy and telecommunications infrastructure in the North Sea (UK signs deal with North Sea countries to protect subsea electricity and oil pipelines, E+T Magazine, 2026). This agreement was a response to growing concerns about infrastructure security.

Infrastructure resilience is essential for energy security. The UK must secure North Sea infrastructure to address holistic national energy security requirements, particularly as the UK has a dependence on interconnected energy systems and offshore energy developments. The requirement for increased infrastructure resilience and security has become more prominent due to recent incidents, such as the 2022 Nord Stream explosions (The Nord Stream Incident: Open Briefing, Security Council Report, 2024). These incidents have changed perceptions of risk, attacks on underwater infrastructure are no longer viewed as highly unlikely events, and recent developments being made are contributing to the protection of underwater systems. For example, UK defence initiatives and underwater robotic systems intended to detect threats and protect cables and pipelines from sabotage (Military-grade underwater robot aims to protect Britain’s offshore infrastructure, E+T Magazine, 2026).

Critical infrastructure failures

Energy infrastructure, alongside reliable network operations, is essential to economic development. Yet, there are infrastructure resilience issues across transmission networks. Addressing these issues will not only enhance resilience, but it will also aid operational transitional readiness as electricity systems become more reliant on power electronics, HVDC links, renewable generation and cross-border interconnection. The April 2025 blackout in Spain and Portugal highlights the importance of this issue. A combination of factors, including system oscillations, and reactive power control, differences in voltage regulation practices, rapid output reductions and generator disconnections in Spain, and uneven stabilisation capabilities, led to rapid voltage increases and cascading generation disconnections, ultimately resulting in a widespread blackout across continental Spain and

Portugal (ENTSO-E Publishes Expert Panel Final Report on 28 April 2025 Blackout in Spain and Portugal, ENTSO-E, 2026). The Iberian blackout should be treated as a case study for the importance for strengthening resilience, monitoring and voltage management and the consequences when these systems fail. These consequences were similarly identified in the Royal Academy of Engineering report (Living without electricity, Royal Academy of Engineering, 2016).

Grid infrastructure

Power system operations necessitate that the energy production and consumption be balanced instantaneously. Failure to address even slight mismatches between supply and demand can compromise service reliability. System frequency is a primary indicator: Where system imbalances cause the grid frequency to change, generation and/or demand require to be adjusted to compensate accordingly to avoid local or more widespread power outages. Power outages can have widespread and serious consequences for individuals and society. Fortunately, there are very few major grid events, but despite removing the risk entirely being impossible, they can be reduced through engineering design and operation. With minimum levels of operational performance defined in electricity transmission and distribution network standards.

The duration, geography, and affected sectors all contribute to the social and economic cost of an electricity blackout; estimates suggest that, whilst extreme and rare, a nationwide blackout lasting 24 hours could cost billions of pounds, loss of life and potential civil unrest. Research found that the UK economy suffered a loss of £17.6 billion in economic output between 2023 and 2024 due to connectivity outages, with the average UK business losing over £11,000 in economic output (Reliability and compensation report: the impact of poor business fibre connectivity, Vorboss, 2024). Power outages could hit services across the economy, with potential to impact national growth knock-on effects to regional economies.

Conclusion

Strengthening the resilience and security of the UK's energy infrastructure is fundamental to maintaining energy security, supporting economic growth and delivering the transition to Net Zero.

As energy systems become increasingly interconnected, digitalised and reliant on renewable generation, resilience must be embedded through a whole-system approach that recognises the interdependencies between physical assets, operational technologies, cyber systems and supply chains. This requires sustained investment in cyber security, workforce skills, digital capabilities and robust response and recovery planning, including stronger requirements for cyber incident response exercises and regular resilience testing.

Utilisation of technologies, such as digital twins, can create advanced monitoring systems and data analytics which can be deployed to improve scenario modelling, support operational decision-making and optimise an increasingly complex energy system that must be both reliable and resilient. Building resilience will also require proactive management of critical assets, investment in network resilience, enhanced voltage and system monitoring, and the adoption of engineering and operational practices that reduce the likelihood and impact of major outages. As the energy transition increases dependence on power-electronics-based

infrastructure and cross-border interconnection, lessons from recent international grid failures should be used to strengthen system security and operational readiness.

At the same time, the protection of national infrastructure, both physical and digital, must remain a national priority in response to evolving security threats. This includes strengthening the security of strategically important offshore assets and subsea infrastructure in the North Sea through enhanced monitoring, international cooperation and coordinated protection measures with neighbouring countries. The UK should also continue to promote cyber security expertise, improve cyber awareness across the workforce, and support the development of robust, transparent and secure AI systems that are subject to ongoing validation and protection from manipulation.

Responsibility for resilience is shared across government, security agencies, regulators and asset owners/operators. By combining strong engineering principles, effective regulation, international collaboration, investment in critical infrastructure, and a culture of continuous resilience improvement, the UK can develop an energy system that is secure, adaptable and capable of supporting long-term prosperity and a successful Net Zero transition.

Contact details

For more information or to arrange a meeting please contact The Digital Futures Policy Team and The Sustainability and Net Zero Policy Team at policy@theiet.org.