Spending Review 2025

About the Institution of Engineering and Technology (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 158,000 members worldwide in 153 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.

Introduction

Strengthening the resilience and security of critical national infrastructure is a key responsibility of the Government, and one that without appropriate measures in place could prove costly for the UK. Although the causes behind outages of national infrastructure can be wide ranging, cyber-attacks have emerged as one of the most prominent threats, and this paper will demonstrate how the consequences of these threats mean that investment in resilience and mitigation planning is vital for the UK's economic security. For example, the UK's energy supply underpins several other sectors, including healthcare, finance and transport. Therefore, cyber-attacks on the national grid would compound several severe impacts, disrupting supply chains and the delivery of financial and public services.

Executive Summary

Key recommendations

- The Treasury should recognise that the use of Artificial Intelligence (AI) in service provision can expose a cyber threat. Money from efficiency savings should be ringfenced to be reinvested into training public service staff and workers across the growth sectors. Government should assess the financial impact of cyber-attack scenarios on critical national infrastructure and growth sectors to target defence investment provision.
- The Government should establish a Chief Cyber Security and Resilience Advisor to ensure government has regular strategic advice on cyber security.
- Departments across government should harness the expertise of professional bodies for guidance, for example, by expanding the expert exchange programme. This ensures we have relevant expertise when it is needed across government and cuts reliance on expensive contractors.
- The Treasury should provide incentives to drive cyber security literacy across growth sector businesses via reskilling and upskilling.

Cybersecurity and AI

With the introduction of Humphrey, the civil service AI support tool, there is considerable opportunity for streamlining processes and increasing productivity. Government estimates

this could free up £45bn that could be reinvested back into public services if AI is utilised effectively across all departments. However, the introduction of AI across government leaves Departments vulnerable to cyber-attacks. The data that algorithms are trained with and used for could be manipulated by a major cyber-attack from the UK's adversaries, manipulating AI algorithms into making the wrong decisions on purpose.

There is no ceiling on the economic harm that a cyber-attack could cause, instead that calculation is based on the depth and seriousness of the attack. The Treasury should recognise this threat and reinvest some of the money saved via AI efficiencies savings into staff training across the growth sectors and in the civil service. Staff training that provides workers with clear examples of what represents a good AI use outcome is critical to ensuring misinformation is not used and perpetuated through the system. This is particularly important as 31% of employers say that artificial intelligence / machine learning will be important to sector growth, but 50% of these employers say they don't have the necessary skills in this area (Source: Digital Skills Survey 2023, IET). It is therefore important that users are AI literate to ensure the protection of economic growth sectors and public services across the country.

Communicating the potential threats and risks around AI will increase awareness, develop competence, and create the correct cyber security culture within an organisation. Senior leaders and managers need to drive cultural change organisationally from the top. Senior management should be incentivised to make awareness and risk management a business priority. As a minimum, every six months policies should be reviewed and updated in accordance with changing environments to ensure that it is relevant and effective as technologies develop. **Government should lead on this by setting an example for its own staff and ensuring funds and time are available to do so.**

Many risk assessments do not include examples relating to cyber-physical systems such as autonomous vehicles. These systems will be susceptible to cyber security attacks and could represent significant risks to the safety of citizens and the economy. **Government should assess the financial impact of cyber-attack scenarios on critical national infrastructure and growth sectors to shape investment prioritisation.** In addition, there is a challenge with systems that use unsupervised learning to localise their responses according to their operating environment. The peculiarities of cyber-physical systems do not appear to be fully addressed. This further justifies the need for the Treasury to support training, so operators are AI literate when assessing performance and risk.

It is important that the UK aligns itself to international standards currently being developed by the British Standards Institution (BSI) and the International Organization for Standardisation (ISO). These standards demonstrate best practice which also outline security and privacy practices for AI use cases. There should be broad awareness and adherence to this across government departments.

Cybersecurity Resilience

The average cost of a security breach for big businesses was around £1.46 million last year. This figure is more than double the £600,000 recorded in 2014. The breach at TalkTalk was estimated to cost as much as £35 million in one-off cost (Source: TalkTalk hack to cost up to £35m, BBC News). With 90% of large organisations and 74% of SMEs reporting information breaches last year, cyber security is more important than ever (Source: Calculating the

reputational cost of cybersecurity breaches, Barclay Simpson). These figures pose a significant risk to businesses which could significantly stifle growth.

The National Audit Office has recently said that the threat to government is severe and advancing quickly, specifically resulting from vacant or temporary positions on cyber security. 58 critical government IT systems independently assessed in 2024 had significant gaps in cyber resilience, and the government does not know how vulnerable at least 228 'legacy' IT systems are to cyber-attack. Attacks on public services can have an impact that goes beyond financial to life threatening. In June 2024, a cyber-attack on a supplier of pathology services to the NHS in south-east London led to two NHS foundation trusts postponing 10,152 acute outpatient appointments and 1,710 elective procedures (Source: Cyber threat to UK government is severe and advancing quickly, spending watchdog finds, National Audit Office). As outlined in this report, skills are one of the biggest ways to protect against attack. However, there is a range of skill levels required, as not everyone needs training to an expert level.

Energy infrastructure resilience

Energy infrastructure outages can have widespread and serious consequences for both individuals and society. The risk of energy infrastructure failing due to AI misinformation or cyber security attacks can be quite significant.

The cost of an electricity blackout to the UK economy depends on factors such as its duration, geographic impact, and affected sectors. However, estimates suggest that a nationwide blackout lasting 24 hours could cost billions of pounds. Research has 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 (source: https://vorboss.com/documents/reliability-and-compensation-in-the-business-connectivity-market.)

These costs come from a mixtures of lost business output, transport disruption, and emergency response. Power outages could hit services across the economy such as finance and banking, retail and e-commerce, and manufacturing - strangling growth and having huge social knock-on effects to regional economies.

To give a few recent examples:

- In August 2019, a power outage caused interruptions to over 1 million consumers' electricity supply. Several other services were disrupted due to the affected service providers' own safety systems or problems with their back-up power supplies. The rail services were particularly affected with more than 500 services disrupted.
- The recent storms in Scotland and Northern Ireland impacted hundreds of thousands of people, shuttering businesses, and taking remote workers offline due to cable damage.
- The Barclays Bank outage between January 31st and February 3rd 2025 left self-employed people at risk of late tax return fines, and businesses unable to process payments

This last example was caused by a glitch but provides a window into what can happen when staff are left playing catch up to cyber outages. If a system blackout lasts more than a few days, the economic damage could reach tens of billions of pounds. There would be supply chain failures, an impact on hospitals, mass business closures, and potential social unrest. **Treasury investment in cyber security and network resilience today, could save billions in lost revenue tomorrow.**

With the potential for AI to monitor and analyse the grid's operations, there is potential for misleading data analysis and faulty decision making. If these systems are fed with incorrect or misleading information, they might fail to identify potential issues such as impending equipment failures or capacity shortages (Source: Policy implications of artificial intelligence (AI), UK Parliament Post). A cyber security attack may also result in a third-party taking control of critical infrastructure, disrupting operations, or gathering confidential information. (Source: NCSC warns of enduring and significant threat to UK's critical infrastructure, NCSC).

With an increase in the number of devices connected by digital networks (Source: Connected tech: smart or sinister?, Culture, Media and Sport Committee) including in energy infrastructure, it exposes these areas to new risks. 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. An AI system manipulated by false data could also open vulnerabilities that hackers could exploit.

To mitigate these risks, it is crucial to ensure that AI systems are robust, transparent, and subject to comprehensive validation and verification processes. The UK can be a leader in AI safety by developing a better, broader, definition of safety and risks of AI tools. There should also be tools and techniques that are available to AI developers that can help them prove they are safe and fit for purpose to regulators. Effective cybersecurity measures are also essential to protect AI systems from manipulation. There is a challenge finding people with the required skills at competitive salary rates. Competency frameworks and lists of recognised qualifications would help provide organisational reassurance over developer competence in particular areas. **Key cyber security roles should have protected status (in the same way as 'medical doctor') to help drive up and guarantee standards.**

Skill shortages

There is a notable shortage of skilled cybersecurity professionals worldwide which leaves organisations vulnerable to cyber threats and data breaches. It is estimated there is a shortfall of over 173,000 workers in the STEM sector: an average of 10 unfilled roles per business in the UK, which is costing the economy a shocking £1.5bn per annum (Source: Government urged to tackle £1.5bn engineering skills shortage through primary and secondary education drive, IET). What is more, 49% of engineering businesses are experiencing difficulties in the skills available to them when trying to recruit (Source: IET skills and demand in industry 2021 survey).

Training costs for cybersecurity professionals can vary widely depending on the level and type of training. Costs can also vary depending on the standard of the qualification - whether it be a basic certification course, more advanced course, undergraduate or post-graduate degree. For example, entry-level certifications like CompTIA Security+ might cost around £400, while undertaking an undergraduate then postgraduate degree course would cost over £40,000.

Investing in good training for cybersecurity professionals is crucial, as it can significantly enhance an organisation's ability to protect its data effectively. In addition, regularly updating skills and knowledge for all employees through continued education and training is also important given the rapidly evolving nature of cyber threats.

The introduction of Skills England offers the opportunity to help tackle this issue. Workers in the STEM sector are in high demand, but we don't have the current pipeline of engineers and technicians with the right skills to fill the labour market – something we have been reporting via our skills survey for the last 20 years, and frustratingly nothing has changed in that time. The 2025 spending review provides a platform for this to change by providing the additional

funding support for upskilling and reskilling in areas of critical importance, such as cyber security and AI.

Focusing on tackling the shortage in the sector requires a dual approach of building a resilient domestic pipeline of engineers and technologists, starting in schools and looking at upskilling and reskilling throughout people's careers, whilst also continuing to attract the best talent from around the world. We cannot effectively tackle the skills shortage in key industries if we are limiting opportunities for growth and failing to attract a diverse pool of engineers and technicians into the sector. (Source: IET responds to UK Government signalling move to curb overseas hiring for tech and engineering jobs, IET)

Systems thinking, resilience, and stability

When considering the balance of efficiencies versus expenditure, the Treasury must consider strategic factors, such as system resilience. Resilience and stability need to be embedded into the different systems. The UK's critical national infrastructure relies on a whole system approach, and negative impacts on one part of the system can have costly knock-on effects throughout the system and economy. Likewise, investment in one area will not necessarily mean resilience across the spectrum. Developing resilient complex systems will play an increasingly important part in people's lives. For example, the power systems extracting energy from wind, sunshine, tides, biomass and fossil fuels, and making it available 24/7 in sockets around our homes. The list of complex systems essential to modern life is long and continually growing, but with the right investment in system resilience and skills, the government can protect the critical national infrastructure systems on which our economy and lives depend.