

Altnets

Developing and Protecting Critical National Infrastructure for the UK's Digital Future

A paper on building infrastructure that is
resilient, adaptable and fit for the future.

Executive Summary

The UK's aspirations for nationwide digitalisation are growing rapidly. How people live, work, and access essential services is shifting due to advances in artificial intelligence (AI), cloud computing, smart cities, interconnected transportation, and the demand for connectivity. However, these developments depend on the integrity of the physical infrastructure that underpins them.

The role of infrastructure providers changes as transportation, electricity, telecommunications, and data centres grow increasingly interrelated. They must take into account how infrastructure is developed, safeguarded, maintained, and upgraded over time rather than focusing on network deployment. The UK's economic strength, the availability of vital services, and the capacity to adapt to disruption are all increasingly bound to network resilience.

For the UK to remain globally competitive, it must not only keep pace with the demand for development but ensure the infrastructure supporting it is secure, resilient and capable of meeting future demand.

This paper examines avenues the UK can take to safeguard its Critical National Infrastructure (CNI), including prioritising enduring infrastructure, safeguarding physical assets, strengthening network resilience and considering the growing value of data and energy sovereignty.

The priority is no longer simply to build fast, but to build infrastructure that is resilient, adaptable and fit for the future.

Chapter 1: Critical National Infrastructure is the Backbone of the Digital Economy

CNI has historically been defined as the physical infrastructure that keeps the nation operational, such as transport networks, energy production and distribution, water supplies, and emergency services. As the UK's economy and society become overwhelmingly digital, the infrastructure sustaining data services and communications has become just as essential to the nation's functioning.

The concept of national infrastructure extends beyond physical assets. It encompasses “facilities, systems, sites, information, people, networks and processes necessary for a country to function and upon which daily life depends.”¹ Increasingly, digital infrastructure sits at the heart of these interconnected systems, enabling the services and economic activity that people and businesses rely on every day.

In 2026, uninterrupted connectivity is a fundamental element of modern life rather than just a convenience. Financial transactions happen in real time, public services are becoming digitally enabled, transport networks use integrated technology to manage operations, businesses utilise cloud platforms and linked systems, and healthcare is increasingly dependent on digital records and communications. Without the infrastructure and physical networks that support them, none of these systems can operate efficiently.

This means that the distinctions between various CNI sectors are becoming ambiguous. Data centres depend on both reliable power and robust communications infrastructure, transport networks call for linked technology to manage operations, telecommunications networks use dependable energy, and energy systems are becoming progressively more dependent on digital connectivity. Therefore, a disturbance in one domain can extend well beyond the specific system that is impacted.

Resilient infrastructure is absolutely crucial to the UK economy. Reliable connectivity promotes business productivity, supports innovation and allows organisations to access the technologies driving the next generation of financial growth. In addition, it connects communities to the larger economy and supports vital public services.

The UK's view of vital infrastructure has shifted, as seen by the designation of data centres as CNI in 2024.² As the volume and importance of data continues to grow, the physical infrastructure required to store, process and transmit it is becoming an increasingly strategic national asset.

It is impossible to isolate the infrastructure that supports the UK's digital economy. The nation's resilience and global competitiveness depend on the development and protection

¹ https://assets.publishing.service.gov.uk/media/5c8a7845ed915d5c1456006a/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf p.5

² <https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/data-centres>

of connectivity, energy, transport, and data, all of which are becoming more integrated into an ecosystem of interconnected infrastructure.

Chapter 2: Why Infrastructure Providers Must Think Beyond Traditional Networks

Infrastructure providers' roles are evolving in tandem with the UK's digital economy. The infrastructure that supports vital industries needs to be viewed as a component of a larger ecosystem as they become more digitally integrated.

The infrastructure of today must do more than connect communities and businesses. It must be able to accommodate new technologies, adjust to shifting demand patterns, and withstand disruptions. Infrastructure providers must adopt a more comprehensive perspective on their networks and the future implications of today's build choices.

This change is especially crucial as connected systems, cloud computing, and AI are now ingrained into the economy. These technologies rely on dependable, high-capacity connections; the speed at which businesses and public agencies adopt and profit from them can be directly impacted by the resilience and quality of the underlying infrastructure.

Infrastructure has a major part to play in addressing regional inequalities. By expanding dependable connectivity outside of urban areas, communities have enhanced access to jobs, healthcare, education, and economic opportunities, thereby reducing the digital divide. Approximately 12% of rural locations lacked access to a basic broadband connection of 10 Mbps in 2020, compared to just 0.4% of urban regions, according to research from the House of Commons Library based on Ofcom data.³

This discrepancy highlighted that infrastructure investment may be increasing overall capacity, but we need to ensure communities across the UK can participate in an increasingly digital economy. In this way, infrastructure investment can support broader regional development and economic growth in addition to network coverage.

Infrastructure is becoming more interdependent; no one industry or provider can handle these issues singlehandedly. Telecommunications companies, utilities, local governments, the UK Government, and other infrastructure operators must work together to deliver forward-thinking CNI, ensuring development and investment are coordinated rather than considered separately.

This involves infrastructure providers accepting more accountability for the part their networks play in the larger infrastructure environment. The goal is to build facilities that support vital services, encourage innovation, increase resilience, and advance long-term economic growth rather than just increasing connectivity.

³ Pattanapong Tiwasing, Beth Clark, Menelaos Gkartzios, "How can rural businesses thrive in the digital economy? A UK perspective", *Heliyon*, Volume 8, Issue 10, 2022, p.2

Chapter 3: Lasting Infrastructure

When infrastructure deployment and installation account for a substantial percentage of the project's total cost, it is especially crucial to get deployment right the first time. Future scalability, maintenance needs, resilience, total cost of ownership (TCO), and continuous operating expenses (OpEx) can all be impacted by decisions made during design and construction. Therefore, adopting a lifetime strategy can minimise needless intervention and future recurring expenditure.

The UK Government advocates a whole-life approach to infrastructure investment, with guidance such as the Facilities Management Plan 2022 emphasising the importance of considering capital, maintenance and service costs across an asset's lifecycle rather than focusing solely on upfront expenditure.⁴

This also means thinking about ways to deploy infrastructure more effectively and with less disturbance. Methods like plug-and-play and pre-connected solutions can streamline and expedite the deployment, installation, operation, management, maintenance, and evolution of telecom services and equipment.⁵

Lasting infrastructure is primarily about generating long-term value rather than it is about meeting short-term demands. For many years to come, the infrastructure constructed today should offer a solid basis for the UK's connectivity requirements.

⁴ <https://assets.publishing.service.gov.uk/media/6364d68ee90e0734627b9cae/GPS-Facilities-Management.pdf> p.19

⁵ Agesen, Finn Arve, et al. "Towards a plug and play architecture for telecommunications." *International Conference on Intelligence in Networks*, 1999. p.332

Chapter 4: Protecting the Physical Assets Behind the Digital World

The infrastructure that supports vital services can be impacted by supply chain interruption, severe weather, fire, physical damage, theft, and sabotage. The increasing connection between digital systems and the physical infrastructure that supports them is highlighted by the fact that cyberattacks can have serious operational and commercial repercussions. This poses a crucial question: how can infrastructure providers strengthen the physical network's resilience?

The scale of the threat is becoming increasingly difficult to ignore. Research into cyberattacks labels the UK “the fifth most targeted country globally for cyberattacks on critical infrastructure”, highlighting the growing pressure on organisations responsible for essential systems.⁶

Critical infrastructure faces a wide range of threats. Physical vulnerabilities can be just as crucial as cybersecurity. Beyond planning for environmental hazards like severe weather and fire, infrastructure providers must safeguard assets against unwanted access, unintentional damage, and intentional interruption.

Cyber Threats

As the UK's digital standing has evolved over the last decade, so has the risk of cyber threats to CNI. The National Security Strategy and Strategic Defence and Security Review 2015 promoted cyber security to a Tier One risk to national security.⁷ More recent high-profile cyberattacks show how rapidly an event impacting digital systems can have broader operational and business ramifications.

After a cyber incident in 2025, retail giant M&S was forced to use manual procedures in several areas of its business and take systems offline after a substantial customer data breach. The business anticipated an impact of almost £300 million on operating profit before mitigation and cited "additional waste and logistics costs, due to the need to operate manual processes."⁸

This emphasises the necessity for holistic resilience, understanding that failures in one area of an increasingly interconnected infrastructure ecosystem have repercussions in other areas.

One strategy to strengthen resilience is to build it into network design from the outset. Redundancy, backup infrastructure, and alternate routes can help prevent significant

⁶ Snider, Hefetz, Shandler & Canetti (2026) Experimenting with Threat: How Cyberterrorism Targeting Critical Infrastructure Influences Support for Surveillance Policies, Terrorism and Political Violence, 38:5, p.516

⁷

https://assets.publishing.service.gov.uk/media/5a7f9d5840f0b62305b88387/2015_Strategic_Defence_and_Security_Review.pdf p.85

⁸ Severino, J., The 2025 Marks & Spencer Cyberattack: Applying the Diamond Model. P.2

disruption in the event of a single asset failure. Therefore, a resilient network is built to continue functioning in the event of disruption.

Smart Access Management

A key, but sometimes neglected, component of infrastructure resilience is physical security. Preventing unauthorised access is only one aspect of protecting network assets; another is making sure that designated people may easily access infrastructure when repairs, upgrades, or maintenance are needed.

Altnets' partnership with [iLOQ](#) illustrates how access management can form part of this wider resilience strategy. Operators can better regulate access to physical assets and lessen the risks associated with lost, stolen, or duplicate keys by substituting remotely managed, self-powered digital locks for traditional keys. When engineers need to access infrastructure, the ability to remotely manage permissions can help shorten wait times.

Overall Resilience

Resilience extends beyond the network itself. Having the necessary equipment, suppliers, engineers, and repair procedures firmly established is essential to being able to react swiftly when a disruption arises. Operational preparedness and supply chain resilience are essential for ensuring continuity and promptly recovering from infrastructure breaches.

Resilience must be taken into account at every stage of the infrastructure lifecycle, from network design and protection to maintenance and restoration, as digital infrastructure becomes more and more vital to the UK's ability to operate vital services.

Chapter 5: How Infrastructure Can Unlock Opportunity Across the UK

Reliable connectivity is becoming a crucial facilitator of opportunity and regional development as digital technologies become progressively integrated into daily life, but not everyone benefits equally from the digital shift.

There are additional barriers to employment, education, healthcare, and business prospects in communities with poor access to high-quality connections. It takes more than just expanding coverage to close this gap. Investing in dependable, scalable infrastructure that can accommodate shifting demand and give communities the long-term connectivity they need to thrive is necessary.

Connectivity as an Enabler of Regional Growth

High-quality broadband connections can help expand economic opportunity outside of the UK's major cities. Reliable networks provide people more freedom to choose where they live and work, allow businesses to function remotely, and provide access to larger markets and talent.

As digital services grow more advanced and data-intensive, investing in robust infrastructure will help guarantee that underserved and rural regions are not left behind. Infrastructure can continue to assist communities as their needs change if networks are built with adequate capacity and scalability.

Supporting Essential Services

The delivery of vital public services is likewise growing far more dependent on connectivity. Reliable networks are essential for connected public services, digital education, and remote healthcare, especially as more services go online.

As a result, connectivity becomes a more general resilience problem. Network disruption has increasingly serious repercussions than just inconvenience when people depend on digital infrastructure to access public services, healthcare, or education.

Connectivity

Connectivity is now seen as a part of CNI, which may help improve not only digital access but also the UK's overall social and economic resilience, as it becomes increasingly ingrained into the country's larger economy.

Building the high-speed, resilient infrastructure necessary for more individuals, companies, and communities to fully engage in the UK's digital future should be the goal, rather than merely connecting more locations.

Chapter 6: Sovereignty, Security and the Future of CNI

Sovereignty is becoming an increasingly important consideration. The UK's ability to ensure confidence and control over the infrastructure, data, and energy that its economy depends on is now more important than just whether it has adequate connectivity or data capacity.

Data sovereignty is at the heart of this debate. Understanding where data is held, who can access it, and whose legal and regulatory frameworks control it is becoming critical as businesses integrate cloud computing, data centres, AI, and linked services. Beyond data protection, data sovereignty refers to the preservation of control over information that may be strategically significant or commercially sensitive.

Data Sovereignty

The need for safe, dependable data infrastructure is rising as AI and data-intensive technologies proliferate. In addition to where their data is physically stored, organisations also need to think about who ultimately controls and has access to it, as well as how changes in geopolitics, regulations, or operations may impact this.

As geopolitical tensions have brought awareness to the strategic necessity of control over digital infrastructure, the significance of data sovereignty has become especially evident. Digital infrastructure may be a part of the broader security picture, as the crisis in Ukraine showed, with the capacity to govern where systems and data are hosted becoming a crucial factor during disruption.

“The 2022 Ukraine conflict established digital sovereignty as a warfighting domain.” The same analysis reportedly found that Russian cyber attacks were significantly less successful against sovereign infrastructure than foreign-hosted systems.⁹

The UK's evolving relationship with foreign data protection regulations also influences data sovereignty issues. In terms of EU data protection, the UK was labelled a "third country" after Brexit, which means that even while its regulations are closely aligned, it is not part of the EU's own data protection system.¹⁰ Questions about the transfer of data between jurisdictions and the applicable legal protections now have an additional layer.

The networks, data centres, and energy infrastructure needed to safely and reliably store, process, and transfer data are inextricably linked to data sovereignty. Infrastructure and information security concerns are a growing necessity, including where data is kept, who can access it, and how securely it can be maintained or transferred. These factors will become even more important as reliance on data centres and cloud services increases.

⁹ فرحات and بن صاف, 2026. Digital Sovereignty: Challenges, Implications, and Pathways for the Future. Algerian Scientific Journal Platform, p. 5.

¹⁰ Celeste, Edoardo, et al. Data Protection and Digital Sovereignty Post-Brexit: An Introduction. Bloomsbury Publishing, 2023. p.1

Energy Sovereignty

A reliable power supply is also essential for data sovereignty. Consistent electricity is necessary for networks, data centres, and digital services, and the interaction between digital infrastructure and the energy system is rising due to the increased demand from connected technology.

The cost, availability, and resilience of digital services can be directly impacted by fluctuations in energy prices or supply disruptions. Data, energy, and connectivity become more intertwined; vulnerability in one can put pressure on the others.

This highlights the necessity for infrastructure providers to think about resilience within the larger infrastructure ecosystem instead of focusing only on specific networks or assets.

Why sovereignty matters for the UK's digital future

The UK's capacity to promote innovation, safeguard vital services, and maintain its competitiveness in a global economy will be impacted by the infrastructure choices implemented today. Therefore, sustaining trust in the UK's digital future depends on building secure, resilient, and integrated infrastructure.

Data sovereignty ultimately depends on infrastructure sovereignty: knowing where data exists, who can access it and having confidence that the physical infrastructure supporting it can be relied upon.

Conclusion: Building the Foundations of a Connected, Resilient Future

The quality of the underlying CNI will determine the UK's digital trajectory. Network infrastructure is no longer just a way to supply broadband, since connection is becoming more and more integrated with energy, transportation, data, and other vital services. It is increasingly contributing to the nation's overall resiliency, both economically and nationally.

Therefore, building infrastructure that can endure disturbance, adjust to shifting demands, and provide long-term value is more important than simply installing more networks. This means taking into account long-term performance, resilience, physical security, and sovereignty in addition to deployment.

For infrastructure providers, this represents both a responsibility and an opportunity. The UK's ability to connect, compete, and react to change in the future will be shaped by the networks being constructed now. Building infrastructure that can support the UK for decades to come, in addition to meeting current needs, must now be the main priority.



www.altnets.co.uk



sales@altnets.co.uk



020 3997 8994



Studio 1, The Boardwalk
Brighton Marina,
Brighton, BN2 5ZB

