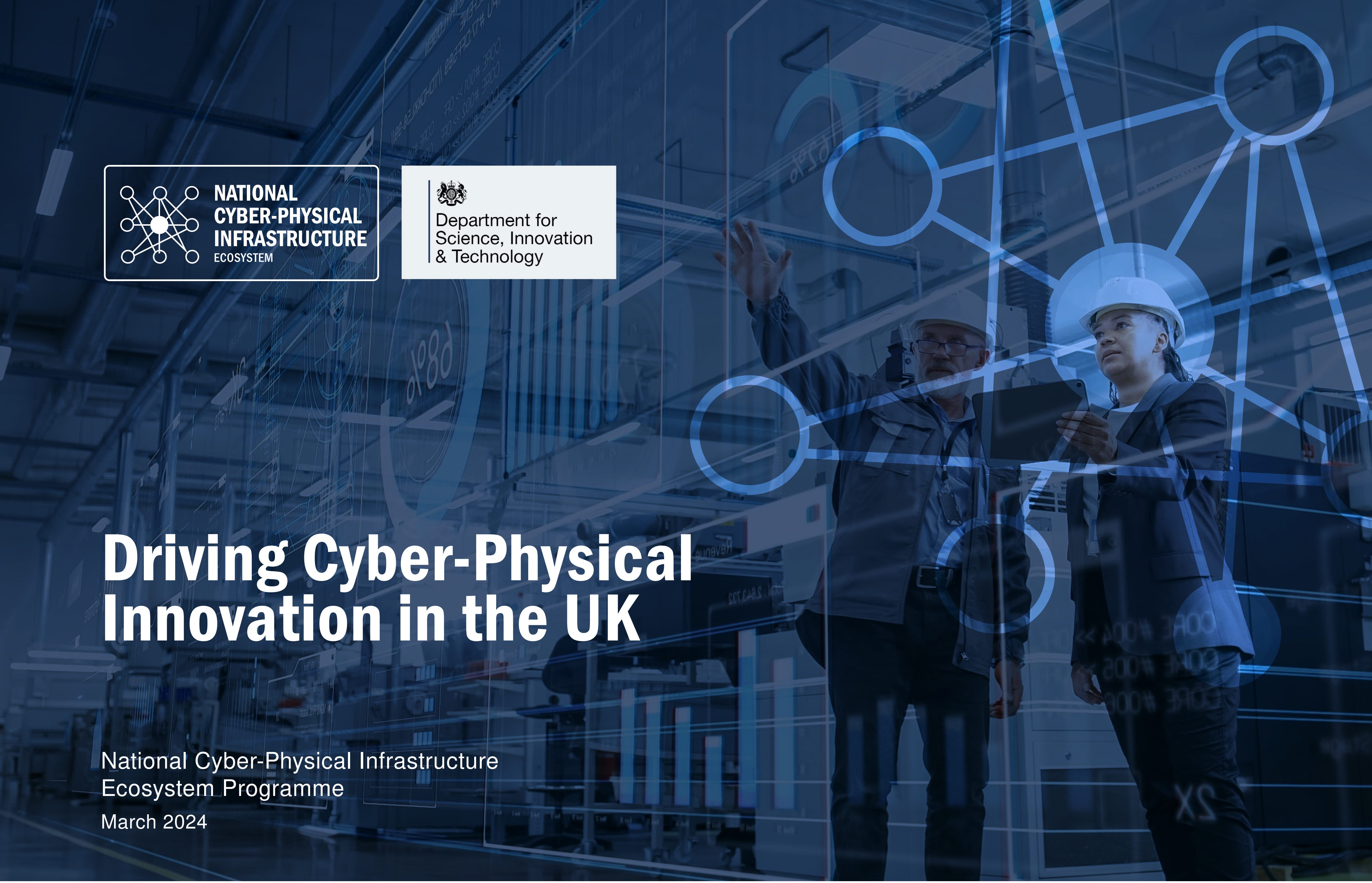


NATIONAL CYBER-PHYSICAL INFRASTRUCTURE ECOSYSTEM

Department for Science, Innovation & Technology

Driving Cyber-Physical Innovation in the UK

National Cyber-Physical Infrastructure Ecosystem Programme

March 2024

CATAPULT Digital

CATAPULT Connected Places

CATAPULT High Value Manufacturing

In brief

Cyber-physical infrastructure (CPI) is the invisible infrastructure which connects the real world with the digital world. It is infrastructure just as roads are infrastructure, and requires planning, rules and regulation to function well, and innovation to function better.

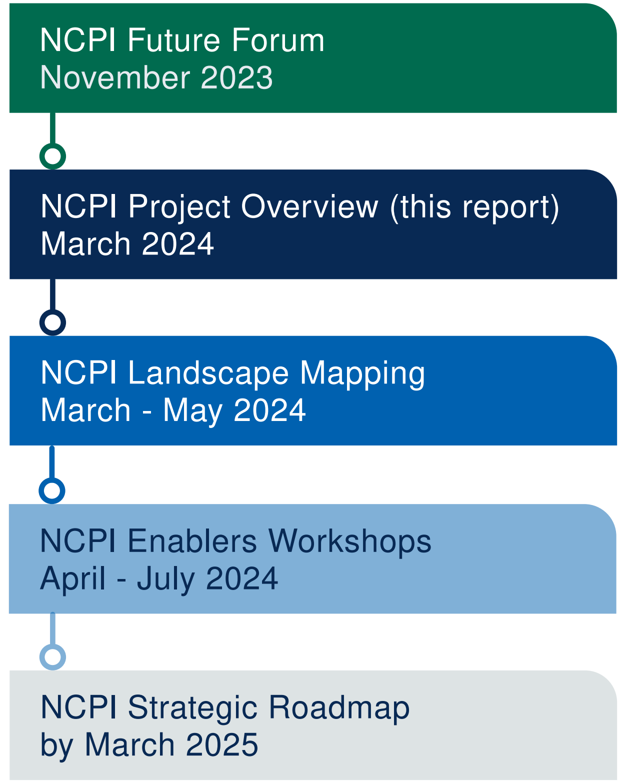
The UK and global ecosystems of stakeholders across the CPI technology stack need to work together to develop this infrastructure in a way that maximises opportunities while protecting UK citizens.

The National Cyber-Physical Infrastructure (NCPI) ecosystem programme marks a starting point in building a coherent collaborative stakeholder ecosystem, working towards a common vision for the future of digitalisation, innovation and the internet across sectors and technologies.

The programme has a number of planned activities involving a range of stakeholders from different sectors and disciplines.

NCPI ecosystem workshops covering enablers and cross-cutting themes will take place across the UK from April to July 2024, with more information to follow.

- April - Cyber-physical infrastructure: key challenges
- May - Security and resilience
- June - Interoperability
- July - Frameworks, standards and guidance



NCPI Future Forum
November 2023

NCPI Project Overview (this report)
March 2024

NCPI Landscape Mapping
March - May 2024

NCPI Enablers Workshops
April - July 2024

NCPI Strategic Roadmap
by March 2025

Introduction

The National Cyber-Physical Infrastructure (NCPI) ecosystem programme aims to establish the UK's position and the seeds of international presence as an innovation powerhouse for connected cyber- physical systems.

The NCPI ecosystem will bring organisations together to develop common goals to address systemic challenges and opportunities across sectors such as net zero.

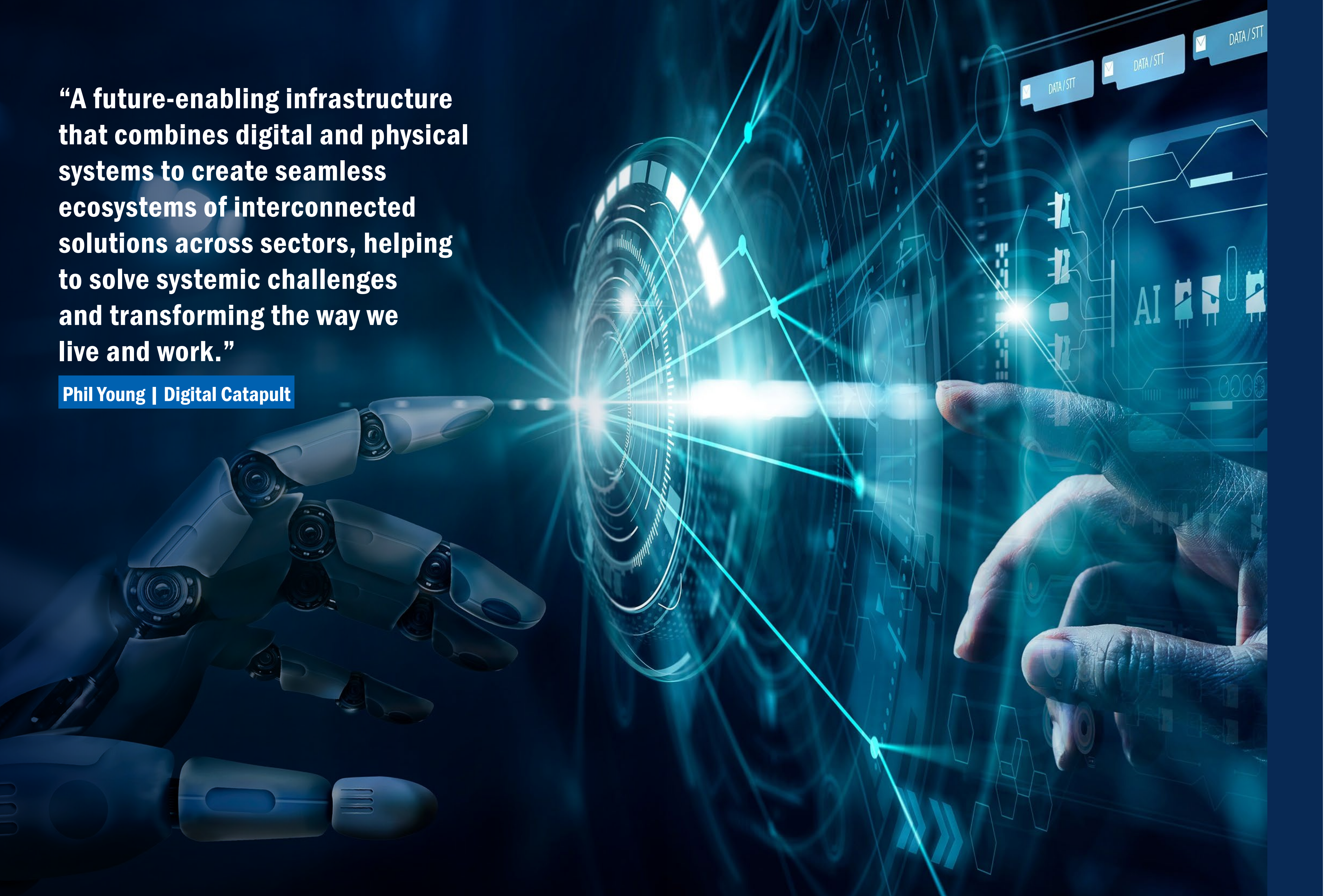
We will ensure we collectively take steps that offer mutual benefits, aligned to greater industry demands, better societal outcomes and continuous improvement.

The UK has substantial expertise in establishing the building blocks for the future in open, interoperable and secure ways - with our history building the world wide web, and our deep science, technology and innovation expertise, we are well equipped to build a cyber-physical infrastructure for the future.

By convening experts into the National Cyber-Physical Infrastructure ecosystem, we can create a vision and a programme that will share learnings, amplify best practices and create synergies towards joined-up cross-sector, cross-technology and cross-disciplinary innovation for how we design, build, develop and connect capabilities such as digital twins, spatial computing / metaverse and robotic / autonomous systems over the next ten or more years.

In this short report, we cover:

1. What is National Cyber-Physical Infrastructure: benefits and challenges?
2. Pathway of activities to setting out a Strategic Roadmap



> “A future-enabling infrastructure that combines digital and physical systems to create seamless ecosystems of interconnected solutions across sectors, helping to solve systemic challenges and transforming the way we live and work.”
>
> **Phil Young | Digital Catapult**

What is National Cyber-Physical Infrastructure?

Cyber-physical infrastructure is the invisible infrastructure that connects the real world with the digital world.

At the National Cyber-Physical Infrastructure Future Forum hosted at Connected Places Catapult on 16 November 2023, Phil Young of Digital Catapult explained the National Cyber-Physical Infrastructure as: “A future-enabling infrastructure that combines digital and physical systems to create seamless ecosystems of interconnected solutions across sectors, helping to solve systemic challenges and transforming the way we live and work.”

We understand the physical world around us as a connected ecosystem of natural systems (natural environment) and built systems (the built environment comprising economic and social infrastructure). The digital world plays an ever-increasing role as the impact of digitalisation rolls out across every sphere of life from healthcare to defence. We are increasingly online and virtual in the way we interact.

Cyber-physical infrastructure is an invisible infrastructure that connects the real world with the digital world. It consists of an underlying infrastructure and products and services that rely on the underlying infrastructure.

Without the creation of this underlying infrastructure where suitable, we limit the prospects for the technological products and services that will emerge if their success is reliant on a small subset of organisations and companies, and we are unable to diversify future cyber-physical system supply chains.

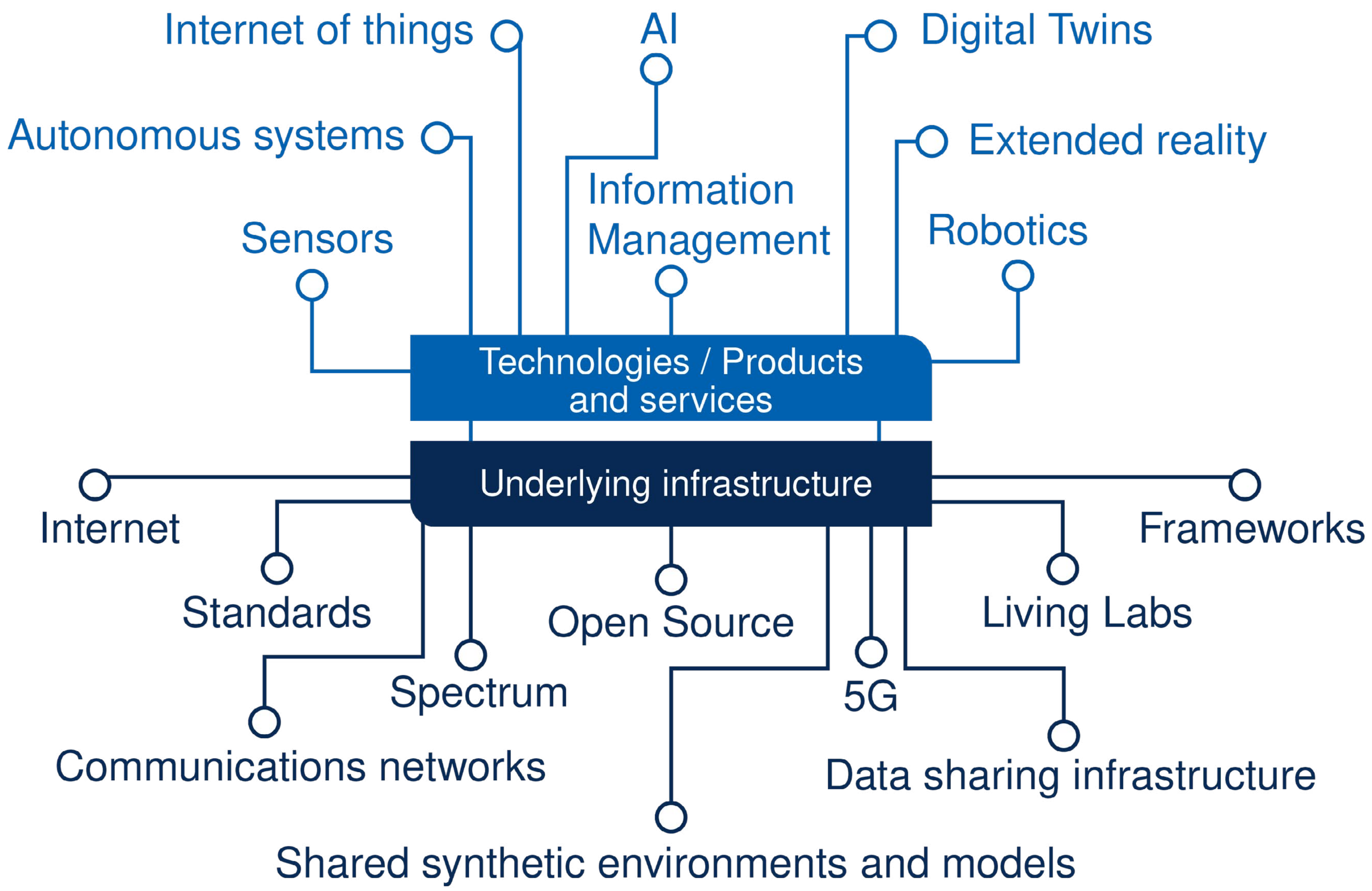


Figure 1. Cyber-physical infrastructure – taking a multi-disciplinary approach to the future of cyber-physical digitalisation

Creating a National Cyber-Physical Infrastructure ecosystem

The underlying infrastructure is part-software and part-hardware and includes but is not limited to systems utilising:

- The internet – a global system of interconnected computer networks that uses agreed rules (internet protocols) to communicate between networks and devices. It is a form of cyber infrastructure.
- Shared synthetic environments and models
- Data-sharing infrastructure[1] (including semantic maps)
- Open-source technologies
- Communications networks (eg 5G)
- Radio spectrum
- Living labs – test zones
- Security and resilience mechanisms
- Decentralised and federated architectures
- Cloud services

The technological products and services that use this underlying infrastructure include but are not limited to:

- Data
- Digital twin technologies[2]
- Robotics and autonomous systems including smart machines
- Artificial intelligence
- Internet of things (IOT) and sensors – the internet of things includes devices and physical things which can communicate with each other through the internet or other communication networks such as wireless networks. IOT uses sensors to gather data and uses a variety of technologies to connect the physical and digital worlds.
- Extended reality (including mixed, augmented and virtual reality), spatial computing and other virtual environments such as the metaverse.

A cyber-physical infrastructure will enable us to get the most out of these technologies by considering how we connect them together, address systems focused challenges and deploy these connected systems into the real world where they can deliver collective value. These technologies can be described as over-the-top (OTT) products and services, which flourish as a result of the underlying infrastructure. Both the underlying infrastructure and the OTT products and services are part of the cyber-physical infrastructure.

1. Elements of data sharing infrastructure described as Trust Prepare Share FSNR workstream 5 consultant recommendations.pdf (ofgem.gov.uk)
2. Digital-Twins.-The-Case-for-Policy-Use.pdf (catapult.org.uk)

Policy and regulation

If the technologies as over-the-top (OTT) products and services are like vehicles, and the underlying infrastructure is like roads then the cyber-physical infrastructure is akin to road transport infrastructure.

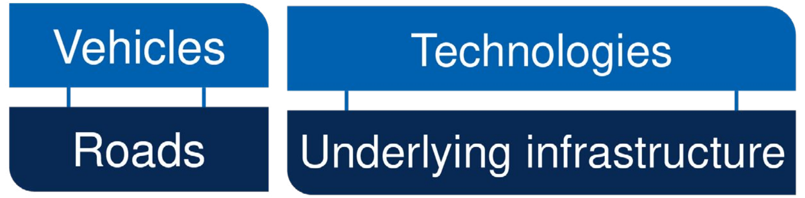


Figure 2. Rules of the road and cyber-physical infrastructure

We know we cannot have functioning infrastructure without rules. We need rules of the road to make the cyber-physical infrastructure work for society and the economy. Both the underlying infrastructure and the OTT technological products and services are part of the cyber-physical infrastructure and need rules.

Equitable access to physical systems underpins UK society. UK law exists to enable its citizens to access the natural and built environments in a way which is fair and reasonable. Anyone can visit a park or a library or use a public road. In 2024, it is not currently the same for digital systems. Digital exclusion is real, Ofcom's 2023 Technology Tracker estimated that 7% of UK households did not have internet access at home.

Cyber-physical infrastructure provides the bridge between physical and digital. But it is an invisible bridge and the reason it deserves attention is because no one can see it. It can evolve and develop in an invisible and nefarious way, so it is essential that the systems and processes around it are as transparent and visible as possible.

Invisible infrastructure can require a greater level of trust to be used effectively. If people don't recognise that trust is missing then using the infrastructure can be unsafe, for example online harms. The internet has evolved without adequate protection in place to ensure that no child is subject to online harm. It is an example of how part of the cyber-physical infrastructure has been left to develop unfettered without rules of the road in place and is now difficult and more costly to make it safe. The prospect of robotics, automation and artificial intelligence puts humanity on the verge of huge opportunities and risks. Invisible infrastructure requires regulation, standards, rules and transparency to function effectively for the benefit of society.

Sovereignty

As an emerging invisible infrastructure, it is necessary to regulate and create rules for the cyber-physical infrastructure. While there is a need for international coordination and to closely follow the work of the European Union, we have an opportunity in the UK to retain sovereignty and shape the future of digital regulation by paying close attention to the need to regulate cyber-physical infrastructure.

Transparency and visibility

The Cyber-physical infrastructure vision[3] set a global vision for the cyber-physical infrastructure, "Tackling climate change will require a holistic cyber-physical intervention at a planetary scale, powered by better tools, smarter ways of working, and greater collaboration and coordination."

"To realise smart machines, we aim to build, connect and populate a new ecosystem of networked virtual and physical collaboration zones. Here, investors, companies, researchers, students, regulators and users can co-create, working together to envisage, design, learn, build, test and manufacture these new tools to act alongside us in the real world."

To enable a virtual and physical collaboration zone, we need cyber-physical infrastructure working for the benefit of society. While ensuring and maintaining cyber security and resilience, everything about the cyber-physical infrastructure needs to be out in the open so that access is as equitable as possible. Cyber-physical infrastructure is infrastructure, and since much of it is invisible, it is necessary to shine a light on its development, rules and use.

[3] Cyber-physical infrastructure - GOV.UK (www.gov.uk)

Enablers

It is up to us to ensure we steer cyber-physical systems towards a positive future for people and the planet.

To enable the development of the cyber-physical infrastructure, which may be largely developed by innovators across the ecosystem, DSIT[4] has identified the following as enablers which Government has a role to foster and promote:

To address these challenges, as a community we need to pool our knowledge and capabilities to create the enabling environment for a cyber-physical infrastructure which achieves the best vision for society.

Security and resilience

Supporting the development of systems that can withstand attacks and failures, both at an application level and nationally, such as systemic supply chain risks

Interoperability

Ensuring different organisations and systems can connect and communicate as easily as possibleagnostic integration, it will ensure substitutes continue to be of low risk.

Recognised value propositions

Supporting the development and communication of the knowledge of how to develop and apply cyber-physical systems and the value they deliver, to facilitate investment

Frameworks, guidance and standardisation

Supporting the collaboration required to develop the common language, approaches and technical requirements for development and deployment, with the subsequent dissemination

Skills

Supporting the development of technical and non-technical skills required to develop a national capability in cyber-physical infrastructure

And as identified in this report: Regulation

Offering clear rules of the road to developers and users of the cyber-physical infrastructure

[4] cpi-consultation-government-response.pdf (publishing.service.gov.uk)

NCPI ecosystem

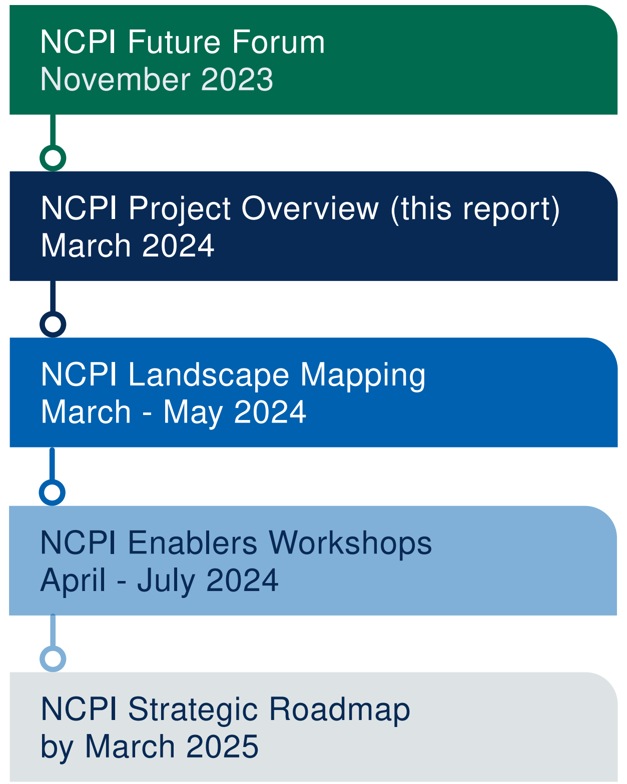
Pathway of activities to a strategic roadmap

The National Cyber-Physical Infrastructure ecosystem building project has been commissioned by the Department for Science, Innovation and Technology (DSIT) and is led by Digital Catapult, the High Value Manufacturing Catapult and Connected Places Catapult including the Digital Twin Hub, in a ‘Catapult consortium’. The project seeks to bring together into one ecosystem the key innovation projects and activities in related areas of cyber-physical infrastructure and the development of complex and connected cyber-physical systems in the UK. It intends to make the case for further interventions and activities in this space. Creating this ecosystem will help to drive industry leadership and support the generation of open best practice, creating a network of shared knowledge and goals – raising national awareness of cyber-physical infrastructure and its importance in our lives.

Objectives

DSIT has appointed the Catapult consortium to promote engagement around the cyber-physical infrastructure ecosystem in the UK. This programme focuses on the enablers identified by DSIT and seeks to:

- Achieve a common understanding of the cyber-physical infrastructure
- Increase transparency and visibility of cyber-physical infrastructure enablers
- Communicate a vision for the cyber-physical infrastructure
- Gain stakeholder input into and consensus around the enablers
- Outline the role for Government.



NCPI Future Forum
November 2023

NCPI Project Overview (this report)
March 2024

NCPI Landscape Mapping
March - May 2024

NCPI Enablers Workshops
April - July 2024

NCPI Strategic Roadmap
by March 2025

Cyber-Physical Future Forum

The Cyber-Physical Future Forum is part of a series of activities to be delivered between 2023-2025, informing a strategic roadmap.

Catalysing innovation – Collaborative workshopping

The National Cyber-Physical Infrastructure ecosystem programme was launched at an event on 16 November 2023 hosted at Connected Places Catapult and online. The Catapult consortium convened stakeholders across industry, academia and government from different sectors as summarised in our article Ecosystem unveiled to better align digital and physical infrastructures. Delegates discussed the enablers and identified key points:

1. **Interoperability** means systems can talk to one another, including hardware and software interoperability. Innovation happens in siloes and requires shared infrastructure to enable collaboration. Governance is required to promote shared infrastructure and collaboration. Governance means agreeing who makes the rules and what the rules are. Competition can damage collaboration and interoperability, so governance is key to developing shared infrastructure and collaboration which then enables competition to produce valued added products and services. Interoperability doesn't happen of its own accord, it has to be purposeful and governed well, enabled by collaboration and funding

2. **Security and resilience** require agreed definitions and metrics. Secure by design is becoming known as a key principle but clear, visible guidance is limited. As the cyber-physical infrastructure evolves, new risks will emerge and we need to understand an acceptable level of systemic risk. As with interoperability, governance and collaboration are crucial to fair decision making and ensuring the cyber-physical infrastructure evolves in a safe way.

3. **Recognised value propositions** can include both financial benefits and social and environmental value. While the business case for individual innovations can be made on an isolated use-case basis, it lacks the true ecosystem value if the innovation is not shared or joined with other innovations or applied to other use cases. This concept of wider social value, or public good, means the incentive to innovate and to provide the underlying infrastructure required to enable the innovation is limited as private investors cannot capture the full value, meaning public funding is required to fill the gap. There is a need to define and measure key performance indicators to better plan and monitor innovation investment.

4. **Frameworks, guidance and standardisation** are required to get the most out of emerging technologies and avoid vendor lock-in. Many frameworks proliferate and it is important to connect frameworks and agree on standardisation and publicise it. Overall technological capability will become greater than the sum of the parts if frameworks, guidance and standardisation are developed collaboratively as part of the cyber-physical infrastructure. Agile frameworks, guidance and standardisation which are coherently connected are required as part of a cyber-physical infrastructure that underpins a changing economy.

5. **Skills** are essential to achieve the full potential of the cyber-physical infrastructure at all levels including at the leadership level. Our capability to develop and use the cyber-physical infrastructure for the benefit of the UK depends upon our choice to invest in and develop a range of skills which span the digital and real-world realms. Digital exclusion will increase if we don't address the skills gap so the range of skills needing to be addressed is broad. At the technical level, if the common elements of the underlying infrastructure are invested in and developed, people will be able to do less of the mundane, repetitive tasks. This might include cleaning up data sets which are required in the absence of a data sharing infrastructure, allowing a focus on more operational and tactical decision making. The skills journey in the cyber-physical infrastructure will be ongoing as we seek to ensure human flourishing.

Future activities

Ideation and strategic roadmap development

Landscape mapping

The cyber-physical infrastructure landscape is broad, and the programme is looking to increase engagement across the ecosystem. The first step is to survey organisations then to map current areas of research and innovation relevant to cyber-physical systems. The Catapult consortium will release a questionnaire, pulling together the resulting data to provide an overview of the National Cyber-Physical Infrastructure ecosystem landscape. This will identify where investment and progress is being made, and help both funders and innovators see where further effort is needed and where we need to coordinate.

The development and evolution of cyber-physical infrastructure needs to be driven both bottom-up and top-down as we as a community need to find the right balance. Too much top-down and we can stifle innovation and creativity, too much bottom-up and the results are uncoordinated and not interoperable – perhaps with greater security risks.

Trying to coordinate a maturing ecosystem is much harder than a nascent ecosystem, and the longer we delay concerted coordination, the greater the cost of interoperability in the future. We need sector convenors to come together to coordinate across sectors. And we need industry's help to identify those sector convenors across the cyber-physical infrastructure, across the areas set out in Figure 1.

Enabler workshops

Cyber-physical infrastructure cannot be developed behind closed doors with the majority of the ecosystem unaware of different initiatives. Its development must tread a careful path between visibility, transparency and security making as much of it as open as possible. The National Cyber-Physical Infrastructure ecosystem programme seeks to bring the development of the cyber-physical infrastructure out into the open and increase engagement with relevant stakeholders.

The Catapult consortium is convening a series of four events in 2024 to enable greater participation across the stakeholder community. These events will enable stakeholders to take a deeper dive into the enablers and the requirements across different parts of the cyber-physical infrastructure ecosystem, building upon the discussions from the Cyber-Physical Future Forum held in November 2023.

Event themes and outline schedule

1. Cyber-physical infrastructure: Key challenges, April 2024
2. Security and resilience, May 2024
3. Interoperability, June 2024
4. Frameworks, standards and guidance, July 2024

These workshops will involve experts across advanced systems discussing priorities within their domains and identifying crossover. The workshops are designed to cover three of the enablers with skills, and value propositions as common themes for each event.

5.

Strategic roadmap

Following the workshop series, the consortium will produce a summary of recommendations and a strategic roadmap for the cyber-physical infrastructure ecosystem, to be published as part of this programme at the end of the year.

Vehicles

Roads

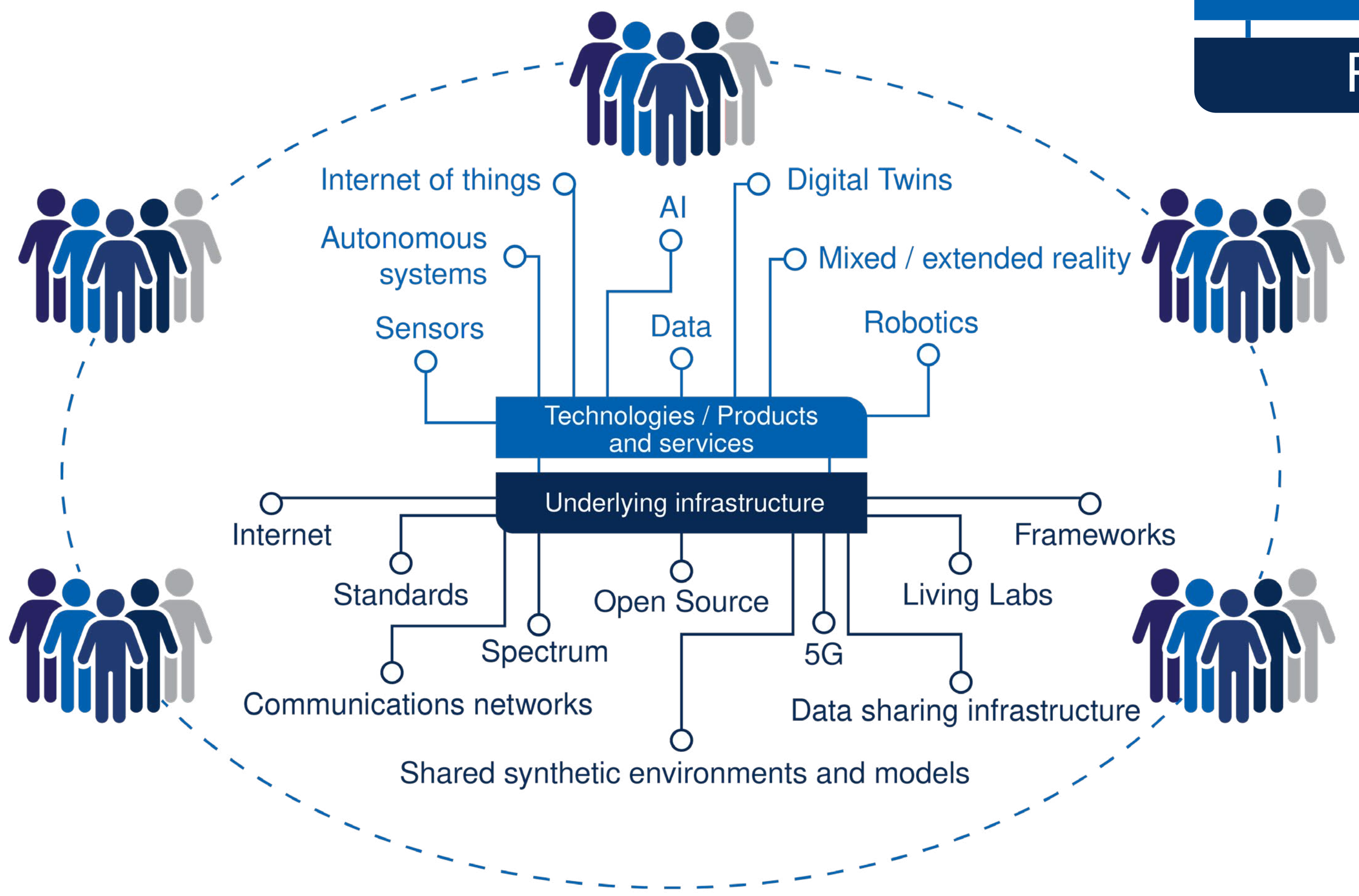


Figure 3. Cyber-physical infrastructure is the invisible infrastructure that connects the real world with the digital world

Information and updates on the National Cyber-Physical Infrastructure ecosystem programme can be found here.

To get involved in one of our workshops or to find out more, please contact us at: info@ncpi.org.uk

NATIONAL
CYBER-PHYSICAL
INFRASTRUCTURE
ECOSYSTEM

Department for
Science, Innovation
& Technology

The National Cyber-Physical Infrastructure ecosystem programme is a government and industry collaboration led by the Digital Catapult, the High Value Manufacturing Catapult and Connected Places Catapult.

Visit our website here

Email us
info@ncpi.org.uk

CATAPULT Digital

CATAPULT Connected Places

CATAPULT High Value Manufacturing