Digital Futures research phase:

Intelligent Digital Fabric

October 2020

The Intelligent Digital Fabric (IDF) is the technology platform that is the foundation of the Digital Futures vision. This paper provides Digital Catapult's support for the Intelligent Digital Fabric based on its own research and the learnings.

Catapult Digital

Department for Digital, Culture, Media & Sport

Contents

Report authors from Digital Catapult

Dr Peter Bloomfield,

previously employed as Senior Policy and Research Manager

Ian Crawford,

Project Manager

Dr Alex Gluhak,

Head of Technology - IoT

Dr Dritan Kaleshi,

Head of Technology - 5G

Dr Casba Kiraly,

Internet of Things Engineer

Dr Alistair Munro,

Senior 5G Advisor

Jessica Rushworth,

Director of Policy and Strategy

Overview

Intelligent Digital Fabric (IDF) is the technology platform that forms the foundation of the Digital Futures vision. It integrates connectivity with service resources as part of a powerful infrastructure enabling current and future digital services in all sectors of our economy.

This paper provides Digital Catapult's support for the IDF, based on its own research and the learnings delivered by workshops with industry and government:

1. Description and visualisation of the IDF
2. Outline of the IDF ecosystem and key players in the UK
3. Use cases
4. Position of the UK in the global market

This paper is an independent report intended to inform the digital environment context for projects funded by the 5G Testbeds and Trials Programme in the Department for Digital, Culture, Media & Sport (DCMS), and also to inform consideration of any future programme covering the development and adoption of technologies, including the internet of things (IoT), in a broader setting.

Here is a summary of recommendations for areas to explore in a development phase of any future programme:

- Agree on a better, 'at scale' mechanism of engagement with industry for more accurate and robust insights, moving from pilots, testbeds and various R&D initiatives to a longer term facilitation of scaled operational adoption
- Security policy needs to be developed and implemented
- Enable longer term facilitation of scaled operational technology adoption to remain internationally competitive and advanced
- Standardisation to achieve interoperability and quality, responding to market pull as well as government push - data, information and knowledge standards are especially important
- It is important that further work is conducted on the resilience of interconnected systems, as this is critical to the five requirements of IDF described in the introduction

Introduction to Intelligent Digital Fabric (IDF)

Intelligent Digital Fabric (IDF) brings together connectivity with a set of service resources (connectivity, sensing, actuation, computation, storage) as part of a powerful infrastructure that is able to support the operation and evolution of current and future digital services in all sectors of our economy. These services will be enabled by intelligent technology for processing, prediction and decision-making.

IDF is an important functional component that digital applications, including IoT, will critically depend on in an increasingly interconnected world, where services in every industry sector become in part or wholly digital. The providers of digital applications may supply elements themselves or they may rely on other providers who supply individual or group elements of IDF. Some examples of future use cases that demonstrate the impact of IDF on the provision of digital applications are set out in the use cases section of this report.

IDF fulfils the following requirements to deliver a wide range of digital services distributed across any sector of our economy:

1. Confidence that services are able to effectively and securely operate in orchestration with each other, to interoperate, interwork as necessary and to coexist
2. Assurance that there is secure exchange and use of information and data between people, services and things
3. Enable exchange of information and data between people, services and things in the real world, to sense their state and influence it
4. Offer easily accessible compute and storage resources, enabling service mobility and edge computing in a time and location-specific manner
5. Enable access to key services, including, for example, artificial intelligence (AI), machine learning (ML) and analytics that extract knowledge from information, and distributed ledger technologies (DLT) that secure the supply chains and workflows

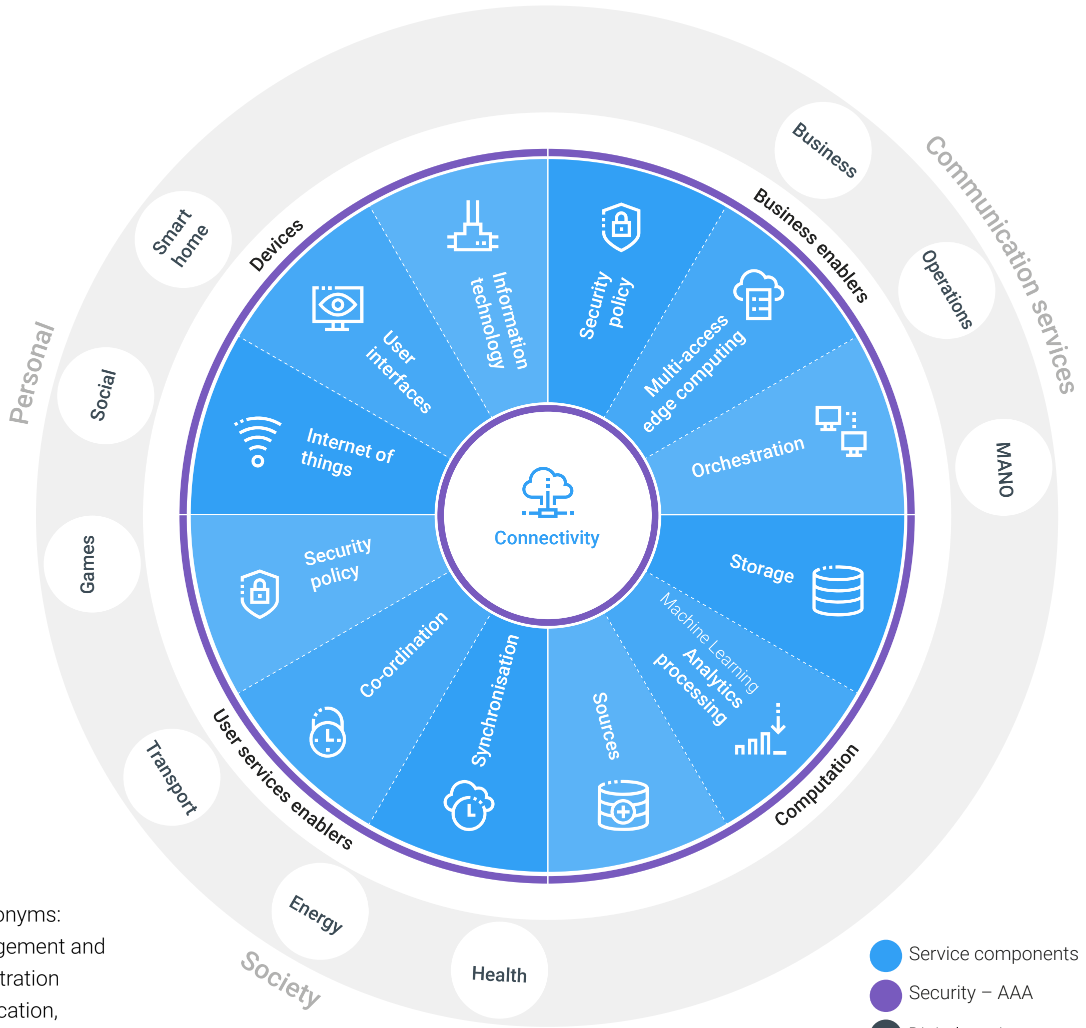


Figure 1

Note figure acronyms:
MANO = management and network orchestration
AAA = authentication, authorisation and access

IDF supports digital services that are linked by a wide range of commercial, personal and societal objectives. Business providers compete to support personal and societal service users.

The representation in Figure 1 has connectivity at its centre. Connectivity means any available type of communications technology that is suitable to meet the requirements of the functions shown in the surrounding sectors, grouped into four quadrants.

This representation is deliberately not layered. Functions in each sector may access functions in any other sector, via an API defined at each security boundary, using connectivity if the information required is remote, or directly if it can be obtained from local resources. For example, functions in the orchestration sector may use machine learning internally via a local API that directly exposes the functions of the analytics/ processing sector, or may access them as a service in a remote cloud platform via connectivity.

Some layered representations are described in Appendix 2 to provide a contrast to the model in Figure 1.

Commercial services and operations (via business enablers) and society (via user service enablers) access the capabilities of IDF via the application of security policies established by qualified authorities (authentication, authorisation and access, AAA). The purpose of these security policies is to protect the IDF and its users.

Commercial services are concerned mainly with the operation and management of connectivity such as the distribution of ICT resources to implement MEC (multi-access edge computing), operations and and management of network slicing for specific customer service level agreements (business).

Personal services are accessed according to security policies established by commercial and non-commercial providers outside the scope of IDF. These policies may be more or less stringent according to the capabilities of the IDF that the services use. For example, smart home functions that are local to defined premises may use some IDF functions under policies set by society providers, but enforce their own policies to protect devices within the premises. Activities that are more people-orientated, such as game-playing, social interactions, social networks and retail, may be constrained in other ways.

A similar AAA gateway opens access to the connectivity component of the IDF. It is separate because the policies implemented by the communications service providers differ from those implemented by providers of digital services for the public, government and enterprise.

The establishment and enforcement of appropriate security policies for the device and computation capabilities are key functions of user service enablers include functions for establishing and enforcing security policies appropriate to the use of information provided by the device capabilities and the computation capabilities. Other functions include co-ordination between multiple parties (maintaining so-called ACID properties - atomicity, consistency, isolation and durability) and synchronisation in time and location.

Business enablers are functions that configure the connectivity of the IDF, ensuring that flows of data are directed to the desired locations (MEC), and that resources are made available in a co-ordinated way (orchestration). Security policies must also be established and enforced.

The devices quadrant and computation quadrant are the technology capabilities of the IDF. In figure 1, data can flow freely between technical and functional components. The functions in the device quadrant are tangible and physical. Those in the computation quadrant are virtualised. For example, networked file systems (the storage function) are commonplace, with the physical electronics that implement them located wherever is convenient and cost-effective for the services being provided and the organisations that are providing them.

The technologies contributing to IDF

The components and functions that make up IDF and the core technologies that are deployed to comprise the full infrastructure are described below.

Devices - A range of sensing and actuating devices enable an interface between the architecture and the environment within which it is embedded. These are devices of any kind that use one or more of the connectivity technologies outlined below. These devices could be physical computers, routers, storage, sensors, actuators, robots, or user interfaces.

Connectivity - This category comprises the diverse range of communications technologies that provide connectivity between the objects and devices deployed in an environment. They include cellular communications (5G, 3GPP release 15 and above, which is backwards-compatible with earlier generations 4G to 2G); short range devices (including Bluetooth, ZWave, Zigbee and others in many spectrum bands), long range systems (often low power, hence 'low power wide area networks' or LPWAN) such as SigFox, LoRa or Weightless; satellite communications; and fibre optics. End-to-end connectivity between devices and computation and storage is likely to use internet protocols (IP) but many of the specifications mentioned use other standards, for example, IEEE 802.15.4 or Bluetooth, and gateway devices that connect non-IP end-devices to IP services.

Computation and storage - Comprise technology that processes and stores data (including data aggregators if they process the data) such as edge compute, data centres, cloud services etc. It creates the information used by digital services via the service enablers, which provide the means (APIs) to do the exchange. Digital services produce information themselves and use APIs to return it to this part of the IDF. The use of RESTful APIs provides an opportunity to adopt a uniform labelling scheme (the URI), that can be used to address individual pieces of information, or devices. The labels can be used to cluster groups of devices, or to ask questions of the information stored in the system. As part of services, information can be made available through a client/server, peer-to-peer, or publish/subscribe interaction model - each has its advantages.

Service enablers - These provide access to specialised backend platforms, for example, Synchronicity Data Broker. They can manage the services delivered by the lower layers and be services in their own right. Examples include: the World Wide Web, the 5G Service Based Architecture (implementing 5G core or a cloud RAN), virtual networks, data brokers and management systems and cloud platforms that provide storage, compute and device management products as a service. These service enablers integrate with artificial intelligence (AI), machine learning (ML) or distributed ledger technologies (DLT) if they need to, and need not have a specific physical location, as they could be implemented in centralised or edge clouds. There are two categories of enabler: one for user services and applications such as transportation, health, or factories; and one for business applications such as MEC or management and orchestration (MANO) to configure the connectivity to meet user requirements.

These deployed technologies form the IDF, and together enable new applications and services to be provided. Multiple components and services can be put together (pick and choose) to form unique product offerings.

Internet of things

The internet of things (IoT) is an emerging domain that is predicted to grow rapidly, bringing together sensors, actuators and advanced applications for consumers and enterprises. There are many communication technology platforms that support IoT, which creates a divided landscape of technology, because of the different demands of the applications and industries that use those platforms. This fragmentation is a barrier to adoption, as potential users, who wish to be flexible without being bound to a single supplier, are unable to make an informed choice and lack confidence that any particular platform is sustainable in the long term.

Many successful consumer IoT use cases are familiar, from voice activated technology, for example, Alexa, to heating and control systems, such as Hive.

However, many economic opportunities around IoT are considered to be in a business or industrial environment, predominantly through productivity and efficiency gains.[1] These can range from solutions for building management and space utilisation (including stock and product management), to measuring processes, predicting faults or highlighting issues in quality or efficiency. While there are many industrial automation systems and communications technologies that are implemented on a large scale in manufacturing industries, these are not generally identified as IoT, and legacy equipment does not use internet protocols (IPs). This is changing, however, as standards and products are enhanced to implement IP.

IoT is a device-based technology that generates state information and events about places, objects and living beings and their surrounding environment in the form of data streams. IoT technology adds connectivity and sensors to everyday objects to add utility, efficiency and value for the benefit of the user. IoT technologies also encompass actuators that are able to influence the state of places, objects, living beings and their environment. This connected layer of devices is evolving and the networks supporting them are changing over time.

Network technology

Connectivity and network technologies underpin IoT, and digital services and are essential for the success of IoT objects (sensors and actuators, for example) in different environments for specific use cases. This section looks at the network technologies currently enabling industrial gains from IoT devices. It is important to consider that network technology is crucial for IoT deployment; however the nature of network and connectivity can evolve over time, hence the detailed explanations that follow are a current snapshot, not the final destination for IoT connectivity.

LPWAN

The availability of suitable connectivity solutions is crucial, as existing wireless (for example Bluetooth or WiFi) and traditional mobile data connectivity (for example 3G/4G) are not able to cope with the demand in scale, coverage, cost and energy efficiency. Emerging LPWAN solutions can provide a suitable IoT connectivity layer in specific, but important, circumstances. For example, in remote or hazardous environments, or where the cost of other solutions would be prohibitive to the business case, and where communication demands are moderate and not delay-sensitive. These forms of connectivity resolve such industry requirements by offering a more cost-efficient means to deploy and operate IoT solutions. The cost efficiencies are achieved by lower costs for connectivity infrastructure and connectivity modules, as well as lower operating expenses for IoT devices in terms of connectivity and maintenance costs.

LPWAN technologies are not just cost-efficient, they also provide a unique combination of low-power operation at devices and long-range connectivity to infrastructure nodes, enabling battery operated devices to be used for several years in large geographic areas, in some cases with national or international roaming capabilities.

LPWAN technologies that operate in both the licence-exempt and licensed spectrum have emerged in recent years. The most well-known examples of the former are LoRaWAN and Sigfox, although other technologies exist as well. By using a licence-free spectrum, these technologies allow simpler deployment models, even self-hosting private networks where a single entity can deploy its own network. Nevertheless, operators providing nation-wide coverage exist in many countries. The latter type, aimed at licensed spectrum operation, represents evolutions of existing 4G networks (for example NB-IoT or LTE-M) to better suit specific communication demands, and is typically deployed by upgrading existing cellular network infrastructure. In the longer term, 5G technologies will enable massive scale IoT deployments for use cases with high bandwidth and low latency requirements, and will also open up the mechanism for delivery of new digital products and services and new and disruptive business models. However, 5G is unlikely to fully replace existing technologies, the current technologies will converge and co-operate with 5G.

LoRaWAN and SigFox network services can handle mobility of devices, including physical motion up to vehicular speeds and roaming between networks. In the case of LoRaWAN, the roaming standard is still in its early stage, with multiple issues and proposals for improvement. Roaming is managed by agreement between providers to accept devices owned by roaming users and assign network and host addresses to facilitate routing between the visited network and the home network, and onwards into infrastructure. It is worth noting that some providers (for example The Things Network or TTN) already have coverage in multiple countries, and mobility in these networks works across borders. In the case of SigFox, there is only one provider partnering with a number of country-specific network operators, thus roaming is always internal to the network, and works seamlessly.

5G connectivity

5G is the term used to refer to the technical specifications (TSs) of 3GPP's Release 15 (and above). To the general public who use smartphones, it will appear to be a more reliable and faster mobile broadband once it has been deployed. From Release 16, due in 2020, there will be an added capability for ultra-reliable low-latency delivery of data (URLLC). This is for applications that require high quality of service (QoS) over a short local distance. It will accommodate a very large number of IoT devices (massive machine-type communications - mMTC). It is backwards-compatible with earlier releases, in particular Release 13 that introduced NB-IoT. As well as a new standard for radio access (called new radio), it redefines the core functions in such a way that they can be implemented as virtual functions in a cloud (the service-based architecture) that communicate using RESTful APIs. It offers a means to integrate network slices supported by software-defined networking (SDN) so that applications using a 5G system can be guaranteed end-to-end QoS. It can be operated easily as a private service, enabling it to be used on the factory floor for mission-critical applications, for example. As with earlier 3GPP releases, it aims to include non-cellular media such as WiFi 6 or WiGiG (operated at 60 GHz over very short distances). The family of TSs that defines 5G is still being developed and the transition from being a 5G service that depends on existing 4G infrastructure (which has a different core architecture, the all-IP enhanced packet core or EPC) to being a stand-alone service will take some time. Deployment of 5G systems that enable IoT services will be complex and costly and will take several years to achieve their potential.

5G is the only platform that supports seamless mobility managed by the network infrastructure; devices can move at up to several 100km/h and can be handed over (for example, passing between channels or points of connectivity without interrupting call or data services) within and between networks. This is an important consideration for transportation and logistics. Service mobility and reconfiguration of network slices is facilitated by the active involvement of the network infrastructure.

Data and artificial intelligence

The infrastructure and services described in this report generate and/or utilise vast quantities of data and information. Recent advances in data processing and storage have enabled commercial growth in artificial intelligence (AI). Three advances have enabled this technology to flourish:

1. access to large quantities of high quality data
2. development of better algorithms to process and analyse data
3. improved storage and computational performance from hardware and cloud computing

These advances have all encouraged newer approaches to AI, such as deep learning and neural network techniques. AI, like other advanced information processing, is intrinsic to IDF. Infrastructure functions may rely on it but also many of the services relying on the IDF will make use of AI, or indeed provide insights or predictions as a service. AI is implicit in Figure 1 in the machine learning, analytics and processing sector for the case where its capabilities are provided as a service via the connectivity core in the way that cloud platforms such as Google and IBM make services available through their APIs.

Cyber security

IDF must be secure by design at all layers, using measures that are effective and maintained for continued effectiveness, and appropriate to the security requirements and safety hazards of the system. The required strength and maturity of the measures will be established by a rigorous risk assessment. Connectivity, particularly wireless media, is vulnerable to physical and electronic attacks that deny service availability, compromise confidentiality, reduce integrity, and corrupt operations (authentication failures, loss of audit trail data). Devices are additionally vulnerable to malware, especially during maintenance. If bogus devices gain access to connectivity then they can create man-in-the-middle attacks. Where there are cyber physical systems deployed, security is a primary concern. Successful device and connectivity attacks will subvert platforms and services, which can be attacked in many other ways. With critical national infrastructure services becoming so heavily reliant on this digital infrastructure, security is a high priority for ensuring national safety and security.

Use cases

The two following use cases describe ways in which the IDF architecture in Figure 1 can enable services and applications in a more joined up manner than is currently feasible. There are many more use cases and potential applications to be built and integrated to IDF across many sectors and areas of society.

Unmanned aircraft system (UAS) traffic management (UTM)

This is a topical use case that has created a high level of interest for many uses of UAS, from delivery of parcels by small drones to mass cargo transport, infrastructure monitoring (road, rail, electricity networks), and urban air mobility (UAM), which is the transport of people by UAS.

People are familiar with drones used recreationally or professionally for filming, surveying and inspection. These are currently resident in the device layer, as complex IoT systems, using various forms of connectivity (type E information flow, Fig. 1.). Industry has ambitions to use UAS for local delivery, long-distance cargo, urban air mobility and agriculture (seeding, spraying, crop management) among many other applications. Where multiple UAS are operated in the same airspace, they must maintain separation from each other and from structures and other local objects and terrain. They can do this autonomously and much more efficiently if they use obstacle avoidance analytics and machine learning co-operatively, combined with external information about airspace traffic, landing spot occupancy, wind speeds in street canyons or weather. This capability is provided by the device and computation layers. To be reactive in real-time, edge computing clouds implement these capabilities, growing and shrinking in capacity as traffic volume changes. Overall co-ordination and management, for example to admit a UAS to airspace, is achieved by the UTM application accessing the other layer functions via the service enablement layer. Where the drone as an object sits in the environment, it relies on communication with the integrated function and action of each technology layer making up the IDF.

Smart metering and demand side management

This is a use case that has a long history going back to the energy crises of the 1980s. There have been, and continue to be, many proprietary remote metering technology platforms, sitting between energy retailers and consumers. Attempts to bring different specifications together, either by central procurement or through consensus between industry actors and government, have had limited success. While not a failure, it is an example of how the use of a network futures platform could provide technology unification and enable new demand-side applications to flourish.

The UK government and energy retailers have worked together for many years to establish a system that empowers consumers to manage their energy consumption and enable retailers to reduce the operational cost of buying electricity from generators. Smart meters in the device layer use available connectivity layer capabilities, (2G, LoRaWAN and local Zigbee relayed through the home broadband router, for example) to supply data to deployments of the computation layer that are implemented by electricity retailers to execute their specific analytics (type A information flow, Fig 1.) and gain competitive advantage by reducing their costs. Smart meters can be exchanged to allow competition between suppliers. Interoperability of smart meters with the enterprise systems of retail energy suppliers can be facilitated by interworking in the computation layer. This could provide a focus for the industry to ultimately eliminate interoperability issues. When a consumer switches suppliers, their credentials, policies, and other data can be moved between the retail enterprises at the computation layer. The computation layer can also manage micro-grids (distributed power plants), exploit edge computing to bring supply back into service after an outage, and organise interactions with the generator marketplace.

UK IDF ecosystem

The technology ecosystems for these different layers are continually growing, particularly for startups and scaleups. This section segments the technologies, outlines the key players in each area and describes their technology niche. It presents the large providers in the network domains, but also some key small businesses developing products and applications. This is a limited cross-section of a much more complex ecosystem. One of the key advantages of a more co-ordinated infrastructure is to provide a lower barrier to entry for startups entering a market, and for industrial players to adopt their technology on their existing infrastructure. The following section outlines the key players in the technology ecosystems already discussed as part of IDF.

Devices

Digital devices provide the interface between the infrastructure and environment. Many of the technologies that businesses use, whether directly or indirectly, will rely on devices. Devices on which individuals and businesses use personal and corporate information technology include computers, laptops, and tablets; wearable devices (including smart watches and sensors); VR/AR headsets, speakers and headphones. But there are also emerging devices, such as smart interfaces for home and business environments. We are familiar with large corporations developing technology in these areas, such as Dell or Lenovo computers, Apple, Fitbit or Garmin watches, Oculus or HTC headsets. However, there are many smaller companies developing device technologies, particularly for uses in industry. Here are some examples of companies deploying device technology for specific industry verticals, rather than in the consumer technology domain.

Wearables:
While Apple and Fitbit are household names, there are many technology companies in the UK, split between medical and non-medical technology. Indeed, the line between lifestyle technology and medical technology is somewhat blurred and consumer understanding and awareness is crucial. Non-medical examples: Elvie focuses on femtech products including silent breast pumps and pelvic exercise devices, while companies such as WaveOptics are producing augmented reality overlays for glasses. Both have received significant investment. Medical examples include: Neurovalens, whose flagship device Modius Health focuses on stimulating the brain's hypothalamus region to improve weight loss outcomes.[2]

Industrial devices: Many IoT device companies make products for an industrial environment, to improve productivity and efficiency to deliver greater insights over processes. Companies such as Total Control Pro introduce tracking devices to a manufacturing floor, to help create efficient movement of products, processes and people. Their use of tracking devices, data and cloud computing-delivered AI solutions helps to improve factory performance. Similarly, larger industrial companies such as RS Components provide IoT development kits for companies to develop their own IoT solutions.[3]

For these companies, it is useful to note that large quantities of data coming from their devices enables a whole range of analytics, ML and AI products and solutions, for example companies like WILD AI, which uses data from wearables to personalise sports and training for women.

Connectivity ecosystem

LPWAN technology is split between licensed and unlicensed networks, and 5G technology is dominated by the large network providers. It is interesting to see that in both unlicensed and licensed LPWAN technology, network providers are developing and rolling out base stations for low powered coverage. There is considerable opportunity for adoption of LPWAN in manufacturing, environment, smart cities, smart homes and health industry verticals. However, successful adoption relies on the rollout of supporting infrastructure.[4] For the unlicensed networks (LoRaWAN and Sigfox) there are two main network rollouts:

LoRaWAN is being deployed in the North East by BT in a collaboration with Northumbrian Water to introduce smart water metering to improve water network performance.[5] The Things Network, a global community with over 100 clusters in the UK, is also a LoRaWAN initiative to support the development of industrial grade IoT solutions from agriculture to manufacturing.[6]

Sigfox is being rolled out in the UK by WNDUK, for which there are currently around 1,900 base stations. The technology is suitable for daily monitoring and could be applied in scenarios where usage of utilities is being monitored.

The licensed network rollout is being led by the large telecoms operators:[7]

NB-IoT (narrow band IoT) is being led by Vodafone, with wide deployment of base stations and connectivity beginning to be available. The map below demonstrates the coverage in the UK for NB-IoT. Wales and the West and South of England have good coverage from the Vodafone network.

The reasons for the current NB-IoT situation are thought to be commercial, requiring agreement between infrastructure providers and mobile network operators.

LTE-M (long term evolution for machines) is being rolled out by O2, with 50 cells deployed currently and a wider rollout scheduled this year. [8]

All these specifications aim for long battery life, and are appropriate solutions for devices that have no other power source for asset monitoring, stock tracking and embedded infrastructure sensors, which are applicable to many industry verticals, from transport to healthcare. However, the actual battery life depends on the device's communications activity. Some protocols are better suited to certain applications than others, but availability of the service is essential. LoRaWAN and SigFox have better coverage at present than LTE-M or NB-IoT. Other criteria must also be considered, such as bit-rate and maximum message length.

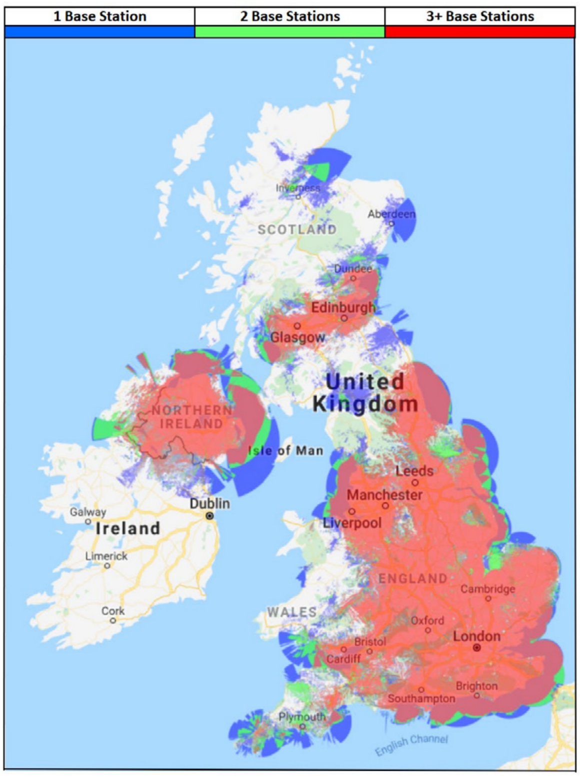
Three has deployed technology for LTE-M, as well as NB-IoT in pilots in the North East, similar to BT's LoRaWAN, focused on utilities maintenance. It has partnerships with Siemens, Northumbrian Water, Northern Gas Networks, Northern Powergrid and Newcastle University, to form the Integrated Transport Electricity Gas Research Laboratory in Gateshead UK (InTEGReL). [9]

There are several market, community and government co-ordinated initiatives to provide more collaboration and utilisation over LPWAN and IoT data. These include, but are not limited to, initiatives Digital Catapult has contributed to, such as Synchronicity, IoTUK, CityVerve, UrbanDataExchange and the Future Networks Lab. As the 5G network is rolled out, there will be convergence of connectivity bands. Some IoT connectivity will transition to the 5G network, while other networks are likely to remain distinct and sit alongside those provided through 5G. The 5G network is being rolled out in the UK by four main players, with each telecommunications provider owning specific bands in the spectrum through auction:

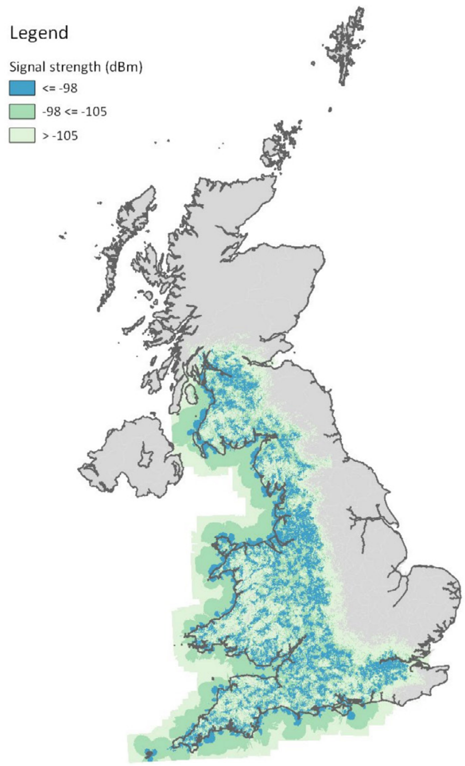
5G players:[10]

- Three 150 MHz
- O2 166 MHz
- Vodafone 226 MHz
- EE 295 MHz

SigFox coverage



NB-IoT coverage



Source: Ofcom Connected Nations Report 2019[11]

Computation and storage

Having large in-house server racks is less prevalent than it once was. The technology enabling IDF, particularly for utilisation of the vast amounts of data being produced, stored, transferred and analysed, is evolving rapidly and becoming increasingly virtualised. With the latest iterations of artificial intelligence technology and machine learning, computation is being approached in a number of different ways.

Cloud compute is a particularly important part of the infrastructure that enables the IDF. The ecosystem of providers is largely globalised, although the data centres enabling the computation and storage is distributed physically as well. In Europe and North America, Amazon Web Services, Google Cloud Platform and Microsoft Azure are the dominant cloud computing platforms. In China, and in a growing global capacity, Alibaba Cloud is a dominant provider.

Chipset/hardware advances have, in part, enabled the boom in AI technology, and chipsets from a range of companies have enabled this. GPUs from NVIDIA (initially graphics cards for gaming, but more recently bespoke hardware such as the DGX-1 and 2) have provided vast improvements in performance. Indeed, much of the cloud computational provision is delivered through DGX, or modified DGX, data centres. With the latest iteration of AI technology, new types of hardware are being created to take novel approaches to computation and distribution of code and process across systems, whether for speed and efficiency, as with the Graphcore IPU, or security and resilience, as with the ARM and Cambridge University CHERI chipset.

Edge compute is difficult to define, with many different descriptions available. For the purposes of AI technology, the edge is considered to be computation closer to the data source, independent of the cloud. Again, with novel approaches to AI, new sectors are developing. Domains such as autonomous vehicles and other automated environments are becoming possible. Collection and processing of data in the source environment is important for safety and efficiency. For example in a factory there may be an AI-enabled safety camera to prevent accidents and allow safer human/machine interaction. The image classification that this device would need to perform would have to take place at the edge, without the latency and processing delays that would happen in the cloud. Some processes can happen seconds, or minutes later, however some cannot afford this delay. Further to this, not all environments where the technology is useful have access to network connectivity. This is where edge computing devices become particularly useful. NVIDIA Jetson is a good example of a small, powerful chipset that can be installed on drones or in areas of limited connectivity to provide computation. The Intel Movidius Neural Compute Stick (NCS) is an example of a task specific device, where an edge device is designed for a specific application - in this case, deep learning inference. Beyond the large providers of compute power already mentioned, Imagination is a UK-based company developing different types of edge computing chips for a range of applications.

Service enablements

The enablements provide a formal, consistent boundary between the functional sectors and their external users. They perform a range of co-ordination and interconnection functions that conceal the complexities of the distributed processing activities and workflows within IDF. From users, enforcing security policies, and, where necessary, exposing the capabilities of the IDF to its users.

There are two categories: one for users accessing services and one for the businesses that create and manage those services on behalf of users.

Users (whether service users or business users) are granted access according to policies defined by digital service providers. A policy states: a means for the user to authenticate themselves (single sign-on, multi-factor, for example); the services that the authenticated user can access or register to access (authorisation, may be chargeable by subscription or usage rate); and the authorised user's ability to read, write or modify information. Such policy-based security and authorisation is commonplace for the cloud platforms mentioned in the previous section. The policy may also distinguish users who have been assigned specific authority: as administrators, system operators or customers, for example. They have a special responsibility to make modifications in co-ordination with other administrators.

The structure shown in Figure 1 is not prescriptive for the definition of such policies. Any provider may define greater granularity that applies to specific types of authorised users. Policies will be defined independently by commercial connectivity providers and digital service providers to the various user communities. They will interact, possibly contradicting each other or being insufficiently detailed, so that they are breached. They, and their interactions, will apply to flows in both directions. Policy quality must be verified to limit such breaches.

It is useful to note: the respective sectors in Figure 1 are identified as 'security policy' for the reasons above. The quality of policies (that they ensure required availability, confidentiality, continuity and integrity) must be verified by the digital service providers and the commercial connectivity providers. Functions in the device and computation categories do not identify a security policy sector explicitly. They will be accessed in general via connectivity, with access having been approved via user service or business service enablers, and with individual accesses validated against those policies as they arrive from connectivity and, again, when the outcomes of those accesses are returned to the initiators. However, local smart home applications that have no traffic via connectivity should implement a similar policy framework.

The other functions in either category are concerned primarily with maintaining a consistent system state. For example, the modifications requested by user, business or operations activities must be validated not just against AAA policy but also with system configuration, for consistency. If the system is provided by multiple entities then any modification must be approved and enacted by all of them in such a way that the entire system remains in a consistent state. If a modification is rejected by any entity then it must be rolled back for all entities. This requirement is often defined in terms of ACID properties: atomic, consistent, isolated and durable; these are necessary properties of distributed interactions, especially ones that incur costs or transfer funds, but also of configuration changes.

The co-ordination, MEC and MANO function sectors must fulfil these requirements: multiple updates to information repositories or device states will be managed by co-ordination; dynamic allocation of edge computing resources by MEC must be done with assurance that the receiving site is able to host the incoming processes and that it is authorised to access their external data; and MANO must ensure that adequate communications resources are available to host new network slices, and release them consistently throughout the deployed IDF.

Synchronisation is more specialised to industrial applications and maintains a uniform time reference and scheduling for workflows throughout the IDF. It is implemented in different ways in different environments, for example on the factory floor, in mobile networks, or by sensors and actuators.

Startup ecosystem

The network technologies described provide the communications and connectivity required to connect the different devices, products and services. This next section will look at some examples of innovative startups relying on infrastructure in different ways:

Iot startups

In the UK, there are approximately 700 startups in the IoT domain, with a combination of hardware, platform and service based products (based on internal Digital Catapult ecosystem mapping). Digital Catapult works with IoT and network focused startups and scaleups through its Future Networks Lab programme of work. The LPWAN network rollout projects and IoT community programmes described in the previous section have helped build a vibrant ecosystem of startups and scaleups, and the products and services of the three companies below are leading the way in IoT solution provision.

VRM TECH

VRM wants to make the housing industry more efficient. This means all participants in the project life cycle collaborating together to decrease costs, increase quality and improve transparency. VRM believes that you can't manage what you can't measure. Its goal is to provide the right data, in the right format at the right time so stakeholders can make informed decisions and create positive change.

pycom go invent

Pycom is an integrated IoT platform with end-to-end solutions that are designed to fit any project. Pycom works with a number of customers to design and develop their connected solutions developing a solution from scratch or putting it all together.

arbnco

Arbnco is a building performance technology company developing disruptive and scalable solutions for the global market. It supplies solutions for human-centric sensing, smart energy and climate change resilience across the built environment, by leveraging our technologies and expertise in IoT, big data analytics, building modelling, AI and machine learning.

AI startups

The AI ecosystem in the UK is large and growing. London is the hub for startups with 770 startups in the capital [12] and an estimated 1,500 UK-wide (based on internal Digital Catapult ecosystem mapping). Digital Catapult works with a large range of AI startups through its acceleration programme, Machine Intelligence Garage. In two years of programme operation, over 100 startups have received technical, business and ethical development support through Machine Intelligence Garage to bring their products to market and build scalable solutions. The programme provides these startups with cloud computing infrastructure and the opportunity to explore a range of computational facilities. A recent cohort was run to explore the crossover between IoT and AI technology and the convergence of these two technical domains. Three companies from this cohort are described below:

For the leading startups dealing with data focused technology, the streaming and storage of data, and access to GPUs and computational resources are of paramount importance. Many of these needs are provided through cloud computing providers as a service model. In the UK, such services are predominantly provided by Amazon Web Services, Google Cloud Platform, IBM cloud services, and Microsoft Azure. For IoT technology, access is relatively bespoke and there are minimal infrastructure level APIs and middleware solutions to provide simple integration between contexts. For many data-reliant startups there is already a considerable overlap in technology domains and an increasing reliance on the IDF infrastructure being described in this report.

NodeNs medical

NodeNs Medical is working to improve patient safety and hospital efficiency, with the goals of improving patient wellbeing, reducing staff workloads, and saving money for hospitals. To do this it has to develop a real-time locating system that uses innovative millimetre-wave IoT sensors enhanced with AI capabilities to precisely track assets around hospitals. The IoT sensors have centimetre-level tracking precision, and smart AI capabilities to detect actions (such as falls) in real-time, without the use of intrusive videos or cameras.

RECYCLEYE

Recycleye is disrupting the waste management industry with an ultra-low-cost, rapidly deployable, decentralised, scalable, digital and fully-automated robotic sorting solution; the Recycleye mini-MRF (material recovery facility). Recycleye has already developed a state-of-the-art computer vision system using recent advances in deep learning and AI, capable of classifying items by material type and brand. The company is developing other technologies that will shape tomorrow's waste management infrastructure and accelerate the world's transition towards a circular economy.

HUMANISING AUTONOMY

Humanising Autonomy is developing a culture and context specific platform for pedestrian intent prediction to improve autonomous vehicles' decision-making, safety, societal acceptance and deployment in urban environments. It envisions a world of natural interactions between people and autonomous systems.

International 5G initiatives

This section assesses the varying approaches to infrastructure to make an international comparison of 5G and 5G use case R&D. This is a good way to look at the funding being put towards connectivity infrastructure and the approach to commercialisation and adoption of innovative solutions and products.[13] The telecommunications industry leaders are providing connectivity, in some cases in a highly subsidised fashion, and the national initiatives in place to drive innovation and adoption of the technology and solutions making use of it. The main UK players were covered in the previous section, however it is worth noting that the UK has a pioneering programme of adoption around 5G infrastructure and technology.

In the Autumn Statement 2016, the UK Government announced its intention to invest in a nationally co-ordinated programme of 5G testbed facilities and trials, as part of over £1 billion of funding announced to boost the UK's digital connectivity infrastructure, including full-fibre rollout.[14]

The 5G Testbeds and Trials Programme at DCMS was set up as a centre of excellence in 2017, to press forward the work in this area. The programme will encourage and fund the creation of a series of testbeds and trials in a range of geographic and vertical market segments. It will explore the benefits and challenges of deploying 5G technologies. It is also interesting to note that the UK is collaborating with South Korea on transport-based use case demonstrations for 5G technology and infrastructure, with both countries committing £1.2 million in funding for the initiative.

China - Launched 5G network in November 2019. Primarily provided by China Mobile, China Unicom and China Telecom as consumer networks. The Chinese government's five year plan in combination with support from Made in China 2025 strategy sets out the R&D and commercialisation support for 5G and related technologies, with sector specific support themes.[15] This comes on the back of significant years of government R&D investments in IoT. According to the GSMA[16], China spent $1.6 billion in IoT R&D in 2014 alone.

Japan - Unusually, Japan is somewhat behind the other players on 5G, with 5G networks launched in March 2020, up to a year behind the front runners. In Japan, the private sector is driving investment in 5G infrastructure, with $14 billion announced[17] from the four leading telco providers. Recent announcements have suggested a tax credit scheme to drive adoption of 5G technology[18], however a national innovation and adoption strategy does not seem to be available. A January 2020 article suggests that Japan may be focusing on 6G more, with $2 billion being used to stimulate private sector R&D.[19]

South Korea - Alongside collaboration with the UK 5G TT programme, South Korea has announced support for 5G use cases and development in the following areas: 'realistic' content, smart factories, autonomous vehicles, digital healthcare and 'smart cities'. They have deployed tax incentives for these sectors to adopt 5G, have 13 testbeds in the country, and are enacting related educational programmes. A regulatory sandbox has been implemented to look at 5G implementation and regulation.[20] SK Telecom is also running a public-private partnership acceleration programme for telecom infrastructure startups. The programme provides funding support, technical support, global networking opportunities and business and innovation support.[21]

Singapore - Beginning in 2020, by 2022, it is expected that 50% of the country will be covered by a 5G network, with the main focus being to implement a standalone 5G network.[22] Unlike in a number of the other leading countries presented here, Singapore is not holding a spectrum auction for ownership. There is a call for proposals where the top two providers will be selected, based on financial capabilities, security of designs and perceived ability to reach 50% coverage by 2022. The criteria for selection are as follows:[23]

- 5G technology trials to demonstrate transformative impact of 5G
- creation of a series of open testbeds to enable research and innovation
- research and development in 5G, for example, cybersecurity

India - As the second largest internet market globally, India has significant trials planned for 5G, with multiple global vendors, including: Ericsson, Nokia, Huawei, ZTE and Samsung. Vodafone Idea is applying for 5G trials with Ericsson and Huawei. Bharti Airtel, with Cisco[24], is seeking permission to conduct trials with Nokia, Huawei and Ericsson.[25] The trials programme appears to cover the infrastructure rollout, but it is currently unclear whether it is combined with industrial trials and innovation support. However, a significant amount of funding has been announced for research and innovation in universities and educational institutes.[26]

Germany - Vodafone Germany and Deutsche Telekom have deployed 5G in 26 cities in total. 1&1 Drillisch has secured the 70 megahertz of spectrum, however its usage will not launch until 2021. Germany is a good example of combining EU funded public-private partnerships for technology adoption with government funded R&D. A programme of government funded R&D testbeds has been set up to trial 5G in sector-specific scenarios, with many examples building on the automotive strengths of the German economy.

The German strategy also outlines a key role in building collaborative consortia for larger corporations to work with startups.[27][28] The 5G Alliance for Connected Industries and Automation (5G-ACIA) is an industry association based in Frankfurt, Germany with international outreach. It aims to ensure the best possible applicability of 5G technology for connected industries, in particular the manufacturing and process industries; that the interests and particular aspects of the industrial domain are adequately considered in 5G standardisation and regulation; and that ongoing 5G developments are understood by and transferred to the industrial domain. 5G-ACIA has published several white papers on the way 5G could be used in the manufacturing industries.

United States - The USA has the most providers of 5G services and infrastructure as part of their rollout. This is from a combination of Sprint, Verizon, AT&T and T-Mobile building most of the infrastructure, and mobile virtual network operator (MVNO) agreements being put in place with other providers across the country.[29]

Testbeds and industry specific use case initiatives feature prominently in many of the national strategies, with funds available to translate from an R&D scenario to a more commercial domain. However none of the strategies or programmes assessed for this report had more targeted incentives to push technology adoption beyond R&D to operational implementation.

5G technology is a good example of how different nations are approaching infrastructure and large scale rollouts of technology that sits as part of the IDF. While many countries have industry testbed and demonstration programmes alongside the built infrastructure programme, the integration with complimentary technologies and enabling widespread adoption appears to be underdeveloped.

Other European activities - The 5G Infrastructure Public Private Partnership (5G-PPP) is a joint initiative between the European Commission and European ICT industry (manufacturers, telecommunications operators, service providers, SMEs and research institutions). It has been implemented in three phases and is presently in Phase 3. Further information about the projects that contributed to 5G-PPP's achievements can be found at Phase 1 and Phase 2. Projects in Phase 3 include infrastructure projects and eight concerned with. Participants in 5G-PPP are generally recipients of EU funding currently under the Horizon 2020 framework research programme.

Opportunities and recommendations

This research has developed an outline of current Intelligent Digital Fabric and how it will develop in the future, increasingly providing the infrastructure required for digital services and products for industry. We have provided an overview of the infrastructure and data flow/communication required, as well as describing the contributing technologies. The operators have been demonstrated for the different forms of connectivity, and some examples of innovative businesses have been provided to demonstrate clusters of services around each technology. 5G rollout has been used as the digital infrastructure use case to understand how different nations are addressing the deployment and adoption of the technology. In the following section we will discuss the opportunities and suggest our recommendations for how best to ensure a scenario is created, which can provide infrastructure for solution developers and industry to make use of to aid productivity and efficiency.

From the research we have conducted and the workshop sessions we have contributed to, we have developed a series of recommendations, which we hope will provide clear areas of exploration in a programme discovery phase.

- IDF considerations need to include both supply and demand, yet only the demand side has been consulted to date. Ongoing development needs to be much broader to incorporate startups and innovative supply chain businesses. There also needs to be a better, larger scale mechanism of engagement with industry for more accurate and robust insights. This should be through a neutral organisation that can interface with industry players, individually and in group discussions, to provide insights and co-designed initiatives.
- IoT policy has been developed around 'secure by design' and is largely consumer focused, although IoT is equally B2B and B2B2C. We believe security in a commercial environment is of equal importance to financial and operational security of businesses. This policy needs to be developed and implemented.
- Pilots, testbeds and various R&D initiatives have proven to be successful in many verticals for the technologies, however there needs to be a longer term facilitation of scaled operational adoption.
- International initiatives around 5G are similar in their approach. For the ongoing success of digital infrastructure programmes, specific initiatives and mechanisms for technology adoption need to be put in place.
- Standardisation is important. There are different forms, for example interoperability standards compared to quality standards. Both are needed for adoption, the former would arise from a market choice, whereas the others need to be government led.
- Data standards are also of vital importance to ensure interoperability of platforms and solutions is considered for the infrastructure detailed here.
- It is important that further work is conducted on the resilience of interconnected systems, as this is critical to the five requirements of IDF described in the introduction.

References

1 https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

2 https://about.beauhurst.com/blog/the-uks-top-wearables-startups/

3 https://uk.rs-online.com/web/generalDisplay.html?id=footer1/release/180828_ursaleo_sensor_uk

4 https://rfdesignuk.com/uploads/9/4/6/0/94609530/murata_lpwan_study.pdf

5 https://business.bt.com/solutions/iot-in-the-pipeline/

6 https://www.thethingsnetwork.org/

7 https://www.ofcom.org.uk/__data/assets/pdf_file/0023/186413/Connected-Nations-2019-UK-final.pdf

8 https://www.ispreview.co.uk/index.php/2020/02/o2-begins-to-rollout-first-uk-lte-m-network-for-iot-in-2020.html

9 https://www.ispreview.co.uk/index.php/2019/10/three-uk-pilots-new-low-power-wide-area-network-lpwan.html

10 https://assets.ctfassets.net/nubxhjiwc091/2aeGqlM3q4m4WW48y6gkOm/d4dba6029fead7538f246ff81b0a5be6/DC_5gMapping_FinalforWeb_Single.pdf

11 ibid

12 https://www.london.gov.uk/sites/default/files/london_theaigrowthcapitalofeurope.pdf

13 https://www.sdxcentral.com/5g/definitions/the-top-countries-with-5g-deployments-and-trials/

14 https://www.gov.uk/government/publications/autumn-statement-2016-documents/autumn-statement-2016#digital-communications

15 https://www.ey.com/Publication/vwLUAssets/ey-china-is-poised-to-win-the-5g-race-en/$FILE/ey-china-is-poised-to-win-the-5g-race-en.pdf

16 https://www.gsma.com/newsroom/wp-content/uploads/16531-China-IoT-Report-LR.pdf

17 https://asia.nikkei.com/Spotlight/5G-networks/Japan-s-carriers-plan-14bn-spending-blitz-for-nationwide-5G

18 https://asia.nikkei.com/Spotlight/5G-networks/Japan-to-promote-5G-with-new-tax-incentives

19 https://www.totaltele.com/504691/Japan-already-developing-a-plan-for-6G

20 https://asiatimes.com/2019/04/south-korea-unveils-national-strategy-for-5g/

21 https://www.true-inno.com/ko/noticeView.do?cSeq=497997d4dfacc05685ee2100a30ed651&strSearchCategorySeq=&strSearchText

22 https://www.rcrwireless.com/20191017/5g/singapore-5g-network-rollout-2020

23 https://www.imda.gov.sg/-/media/Imda/Files/About/Media-Releases/2019/Fact-Sheet-5G-Innovation.pdf

24 https://advanced-television.com/2020/03/09/indiacisco-airtel-to-launch-5g-ready-network/

25 https://economictimes.indiatimes.com/industry/telecom/telecom-news/govt-will-give-5g-spectrum-for-trials-to-all-players-prasad/articleshow/73033442.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

26 https://eandt.theiet.org/content/articles/2019/08/view-from-india-5g-promises-leapfrog-opportunities-for-india/

27 https://www.bmvi.de/SharedDocs/EN/publications/5g-strategy-for-germany.pdf?__blob=publicationFile

28 https://www.techradar.com/uk/news/whos-winning-the-race-to-5g

29 https://www.lifewire.com/5g-availability-us-4155914

Digital Catapult is the UK's leading advanced digital technology innovation centre, driving early adoption of technologies to make UK businesses more competitive and productive and grow the country's economy.

We connect large established companies, startup and scaleup businesses and researchers to discover new ways to solve big challenges in the manufacturing and creative industries. Through this collaboration, businesses are supported to develop the right technologies to solve problems, increase productivity and open up new markets faster.

Digital Catapult provides physical and digital facilities for experimentation and testing that would otherwise not be accessible for smaller companies.

As well as breaking down barriers to technology adoption for startups and scaleups, our work de-risks innovation for large enterprises and uncovers new commercial applications in immersive, future networks, and artificial intelligence technologies.

For more info please visit: www.digicatapult.org.uk

To keep up to date with Digital Catapult's latest work please subscribe to the newsletter here