Grant Agreement N°: 825082
Call: H2020-ICT-2018-2
Topic: ICT-27-2018-2020, Internet of Things
Type of action: CSA

Next Generation Internet of Things

Deliverable number	D3.1
Deliverable title	IoT research, innovation and deployment priorities in the EU White Paper
WP number	WP3
Lead beneficiary	MARTEL
Deliverable type	Report
Dissemination level	PU
Delivery due month	M18
Actual submission month	M22
Authors	Pasquale Annicchino, Anna Brékine, Federico M. Facca, Adriënne Heijnen, Francisco Molina Castro
Internal reviewers	Adriënne Heijnen, Martin Brynskov
Document version	1.0
Project start date	01.11.2018
Project end date	31.10.2021
Duration in months	36 months

This deliverable is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 825082.

Executive Summary

The "IoT research, innovation and deployment priorities in the EU White Paper" presents preliminary recommendations for the coming Multiannual Framework. The priorities and the linked roadmap build on the market analysis conducted on the outcomes of the stakeholders engagements (covered by the advisory board and the different workshops organised by NGIOT project).

Key enablers identified in the discussions with the stakeholders are:

- Edge Computing
- 5G
- Artificial Intelligence and analytics
- Augmented Reality and Tactile Internet
- Digital Twin
- Distributed Ledgers

These key technology enablers are fundamental to support the priorities identified for IoT evolution and adoption. Key priorities identified so far are:

- **R1 Reliable, low-cost, sustainable and scalable IoT networks.** This priority deals with the challenge of increasing the capacity of IoT networks while reducing their deployment costs.
- **R2 Next Generation IoT data processing architectures.** The large decentralisation of IoT networks and the advent of edge computing challenges current data processing architectures. This priorities deals with the need for adapting or re-designing such data processing stack (from the hardware to the software).
- **R3 Futureproof security and trust.** Trust toward IoT is still one of the barriers hindering its adoption. This priority focuses on increasing trust toward IoT by increasing security self-healing capacities of IoT infrastructures and by increasing the scalability of traceability solutions for IoT data processing and sharing.
- **R4 IoT, processes, and data Interoperability.** The plethora of sensors, protocols, platforms and applications is increasing the complexity of integrating different solutions. This priority deals with the challenge of increasing interoperability.
- **R5 IoT, Citizens, Privacy-by-design, and Ethics.** IoT is more and more pervasive in every aspect of our daily life. This poses different concerns regarding privacy and ethics. This priority focuses on ensuring that citizens can easily control privacy and that their privacy is preserved while data generated by their devices is processed.
- **R6 Real time decision-making for IoT.** The increasing number of data generated by IoT devices and platforms, and their decentralisation in a cloud-edge-distributed architecture is challenging real time decision capacities. This priority deals with advancing real time decision capacities and ensuring that such decisions are understandable and trustable.
- **R7 Autonomous IoT solutions.** IoT large scale deployments are still rare in Europe and globally. The complexity of an IoT solution is such that without increasing automation, costs of large scale deployment will be difficult to sustain. This priority covers the need for increased automation in IoT solutions (from devices and edge gateways to core IoT infrastructure services) so as to simplify their management and facilitate the deployment of large infrastructures.
- **R8 Human and sustainable development in the loop IoT.** IoT may play a central role in improving the quality of life of European citizens. This priority focuses on increasing the support of IoT solutions for human interaction while increasing their sustainability so as to ensure coherent contributions to sustainable solutions based on IoT technologies.
- **R9 IoT data sharing and monetisation enabling models and technologies.** While the amount of data generated by IoT devices is increasing, limited data are publicly available. This priority

deals with increasing the size of IoT data market through incentives, best practises and more mature technologies.

- **R10 Sustainable and biocompatible devices.** Sensors and edge devices are an essential element of IoT systems and recent research in the area of bio-electronics and energy storage have the potential to increase their life span while reducing their environmental impact. This priority focuses on increasing energy autonomy of devices and bio-compatibility of sensors.

Contents

List of Figures

List of Tables

1 INTRODUCTION

1.1 Scope

The "IoT research, innovation and deployment priorities in the EU White Paper" aims at synthesising insights from key resources in the complex and wide area of IoT as input to the European Commission (EC), EU member states and other stakeholders when shaping upcoming initiatives, including research, innovation and implementation programmes in the EU Multifinancial Framework (MFF). It particularly, but not only, intends to provide a first set of priorities for the upcoming Horizon Europe and Digital Europe programmes that emerge from trends, ambitions, challenges and needs gathered within the IoT community, including the research community, European industry, policy makers, public sector, regulators and other relevant stakeholder organisations and individuals.

This white paper aims at supporting the European Commission, member states and other stakeholders to:

- Prepare for and lead the development of next generation IoT, as part of a Europe Fit for the Digital Age.
- Identify research, innovation and implementation priorities and challenges for future public (and private) investments (e.g., defining future work programmes and calls).
- Reinforce the EU's digital capacities (computing, data, cybersecurity, AI, skills, interoperability etc.) in industry and the public sector.
- Support the Digital Single Market vision and plans, linked to prosperity on the local community-level.
- Maximise societal, economic and environmental benefits, including roll out and adoption.
- Ensure Privacy-by-Design technology and addressing end-user acceptance.
- Build a world-leading connectivity infrastructure.
- Strengthen and further mobilize the European IoT community and ecosystem.
- Support creators and ensure the widespread distribution of their works.
- Help maximise Europe's progress toward the Sustainable Development Goals

1.2 Methodology

The work leading to this white paper has been organised to create and deliver meaningful insights and recommendations for public and private investments.

This required an initial definition of an agile and effective methodology to allow the extraction of valuable information from the many sources available online and offline, while maintaining close coordination with the European Commission (with direct rapport to the IoT Unit at DG Connect, but linked to initiatives widely across the EC) and dealing with a quite challenging timeline. The work was organised as follows:

- **Bootstrapping & Set-Up**. In the first months of the NGIoT project, we met the EC representatives and several other stakeholders in the IoT LSP arena, also via dedicated IoT LSP Activity Groups engagement, so as to identify relevant stakeholders/people/projects to interact with, as well as to identify relevant information (pre-existing documents, market

reports, articles, etc.) and liaise with relevant initiatives (IoT LSP, IoT Forum, AIOTI, IoT Security Cluster, OASC etc.)

- **Information Gathering** has gone through two main channels: online and offline in order to create a solid knowledge base. Key resources include:
  - Research and strategy reports resulting from IoT projects and initiatives. Additional resources include material presented at the kick-off meeting and at dedicated events, such as the IoT Week in June 2019 and workshops on a variety of topics, from marketplaces to procurement,
  - Stakeholder and expert input from targeted dialogues/interviews online as well as at relevant IoT conferences, workshops and webinars[1],
  - Feedback from the NGIoT Strategy Board[2],
  - Consultation of the broad community of researchers and innovators, via the online "IoT Research and Development Survey" run by NGIoT from March to July 2019.
- **Analysis Phase**. Information collected from various sources contributed to the analysis phase, which ran through several iterations and aimed to extrapolate insights regarding the main priorities and challenges to be faced for larger and more impactful development and adoption of IoT concepts and technologies, the major impact to be expected, especially at the economic level, and the main vertical market segments that are of utmost relevance for better targeting future public (and private) investments.
- **Validation Cycles**. The validation phase involved the NGIoT partners, Strategy Board, experts and several EC representatives. This allowed the original scoping paper delivered in September 2019 in the current document. Further validations will contribute to the next version of the white paper.
- **Outreach Phase.** The white paper will be widely distributed and promoted across the various NGIoT channels, after the next round of validation with the EC and improvements will be made as needed. This will be the basis for further consultation and co-creation processes, run in conjunction with the NGIoT Strategy Board, expert groups and other stakeholders. The information in this document is synthesised to help define the scope of the future research, innovation and implementation priorities for the European Commission, member states and other stakeholders considering the relevance and potential of the various challenges ahead.

[1] NGIOT. D3.2 - Future Trends in IoT (2020)

[2] NGIOT. D1.1 - Ecosystem Building Vision and Report (2020)

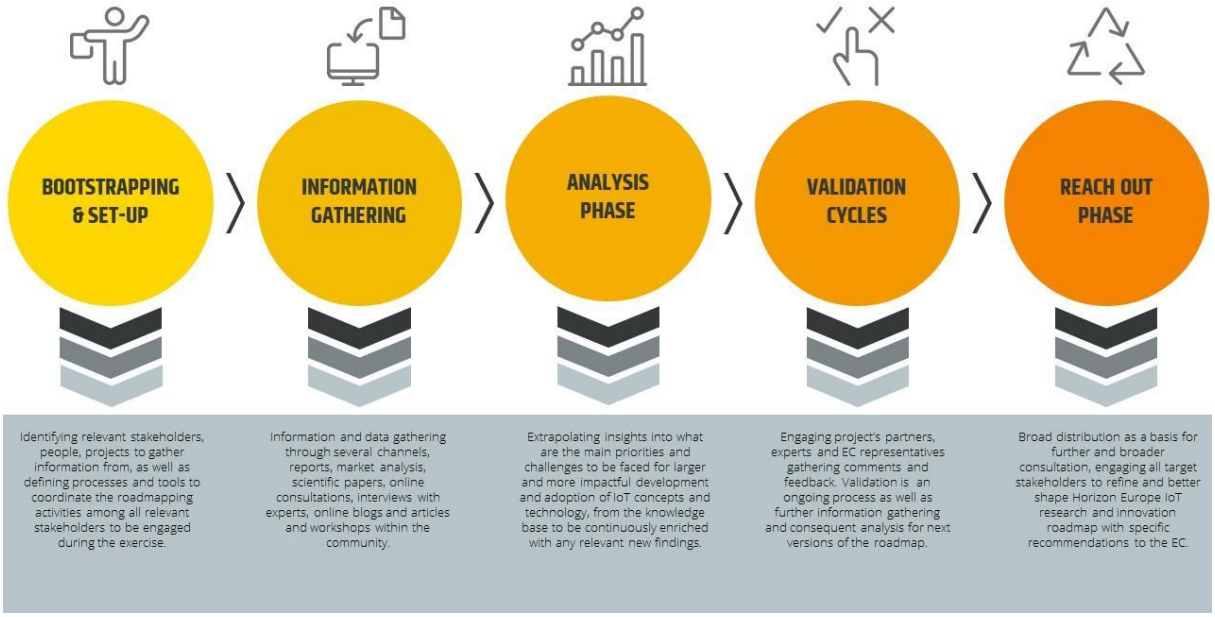


Figure 1. WhitePaper Methodology

2 WHAT IS IOT?

Defining a technology is not easy: different stakeholders put accents on different aspects, or again, the definition of a technology may evolve over time with the evolution of the technology itself. Of course this applies as well to the "Internet of Things" (IoT): its architecture, functionalities and goals today are surely not the same of when Kevin Ashton coined the term "the Internet of Things" in 1999 to link Radio-frequency identification (RFID) technology to Internet.[3]

IEEE in 2015 launched a community effort to "contribute to the ever changing definition of IoT"[4], that resulted in the following definition[5]:

> "Internet of Things envisions a self configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration."

The IEEE community definition attaches to IoT a number of capacities that are desirable, but not necessarily characteristics of most of the IoT systems. For example, several IoT solutions (today) are not self configuring, neither use standard communication protocols, or are available anywhere, anytime.

The International Telecommunication Union (ITU), one of the main Standard Development Organisations (SDOs) in the field, provide a more generic definition of IoT[6]:

> "The Internet of Things (IoT) is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."

The same recommendation (ITU-T Y.2060) define a thing as: "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks".

ITU definitions offer a good base, and highlight a key aspect of IoT not discussed in the IEEE definition: **nowadays IoT, in its wider notion, is not a technology per se, but rather a combination of existing technologies that evolved thanks to things-enabled applications' requirements**. Though, compared to the IEEE definition, ITU definition does not explicit the dual interaction that IoT supports with things, i.e. metering and actuation, which is essential to provide advanced applications. Probably ITU puts also too much accent on the "global" aspect, while in some scenarios IoT may actually be very local (especially taking into consideration the growth of edge computing adoption). As a remark, none of the two definitions stress the fact that **the IoT infrastructure is composed by heterogeneous and**

[3] Ashton, Kevin. "That 'internet of things' thing." RFID journal 22.7 (2009)

[4] IEEE IoT Technical Community, https://iot.ieee.org/definition.html (2020)

[5] Minerva, Roberto, Abyi Biru, and Domenico Rotondi. "Towards a definition of the Internet of Things (IoT)." IEEE Internet Initiative 1.1 (2015): 1-86.

[6] "Overview of the Internet of things" ITU Recommendation ITU-T Y.2060 (2012)

widely distributed hardware and software components. This, according to NGIOT and experts involved by the project, is a key aspect of IoT.

Finally, the range of applications targeted by IoT is very heterogeneous spanning from B2B sectors, such as industrial automation, to B2C ones, such as home automation. This **variety of scenarios implies that there is not a single reference architecture that can be applied to any application, but rather there are a set of characteristics functionalities that are in general typical of an IoT system**. As a consequence, each specific IoT application leverage only the specific functionalities required for its realisation.

In short, we can define the Internet of Things as a systems of systems[7] that have (at least) the following properties:

- **Sensing and actuation**: things, thanks to different components part of the system, can be measured and controlled.
- **Connectivity**: things and the other components part of the system are interconnected, mostly over Internet protocols (but not necessarily).
- **Intelligence**: data collected from things are aggregated and analysed to derive knowledge to present it to users and to actuate things accordingly.
- **Heterogeneity**: devices in IoT are based on different hardware platforms and networks. Similarly the software components composing the system may be highly heterogeneous to be able to serve the different needs of different scenarios and users.
- **Dynamicity**: devices and other components of the system can change over time, so the data they produce and receive (in term of format, scale, and frequency).
- **Scalability**: the number of devices that communicate and the amount of data generated may be enormous for large IoT deployments, or where data frequency is high.
- **Security**: vulnerability of devices and components part of the system may expose the system to critical security issues, that may have an impact beyond the single affected device. Thus the whole system needs to be secured and resilient to security attacks.

In the following sections, based on reference literature, we depict typical IoT systems architecture and we briefly discuss application scenarios.

2.1 IoT Architecture

Several organisation and projects worked on the definition of reference architectures for IoT systems, including, for example, IoT-A[8] and Large Scale Projects[9] (European Funded projects), WSO2[10] and FIWARE[11] (open source projects), AIOTI, ICC (Industrial organisations) ISO[12] and ITU[13] (Standard

[7] "an integration of a finite number of constituent systems which are independent and operatable, and which are networked together for a period of time to achieve a certain higher goal". Mohammad Jamshidi, Systems of Systems Engineering: Principles and Applications (2009)

[8] Bauer, Martin, et al. "IoT reference architecture." Enabling Things to Talk. Springer, Berlin, Heidelberg (2013). 163-211

[9] LSP. IoT Pilots Architectures (2020)

[10] WSO2. A reference architecture for the Internet of Things (2016)

[11] FIWARE. Catalogue (2020)

[12] ISO. "IoT Reference Architecture", ISO/IEC CD 30141 (2018)

[13] ITU. "Architectural reference models of devices for Internet of things applications", ITU Recommendation ITU-T Y.4460 (2019)

development organisations). Some of them, like the Industrial Internet Consortium[14], RAMI[15] and Synchronicity[16] are connected to specific domains. Defining a new reference architecture is out of NGIOT's scope. Large Scale Pilots have consolidated their effort in an interesting 3D reference model (cf. Figure 2) that combines architectural layers, non-functional properties and cross-cutting functions.

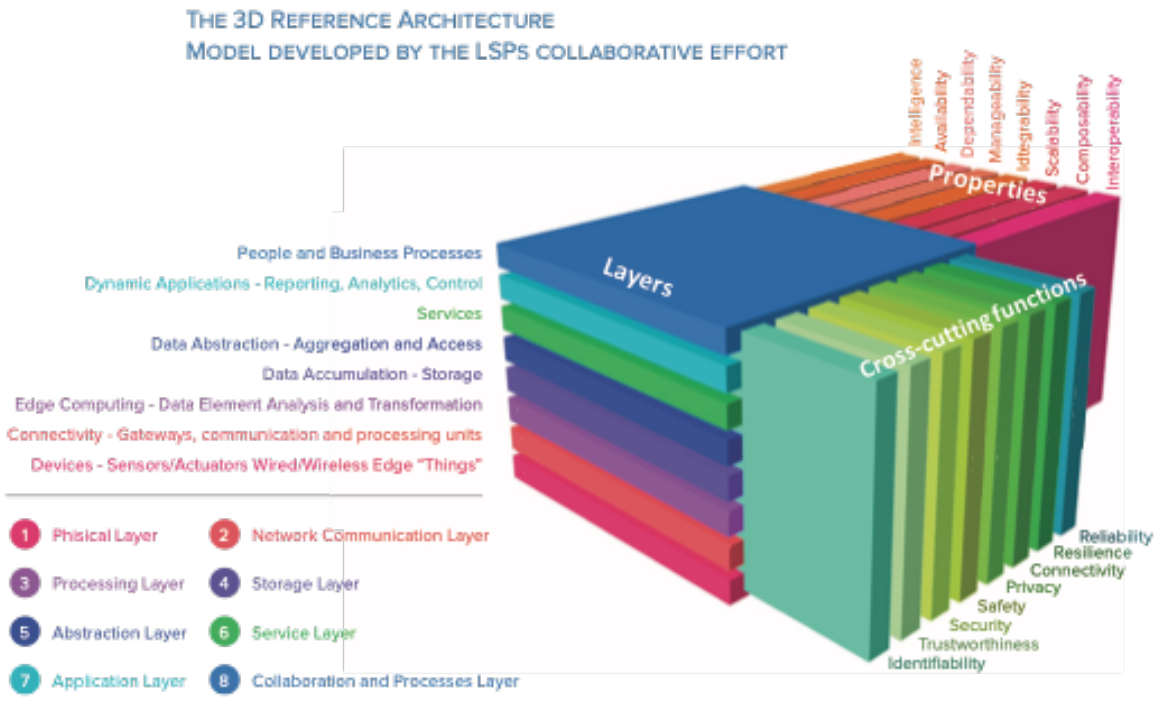


Figure 2. LSP 3D reference architecture

The **Physical Layer** is composed by devices that link the real world to the IoT system by collecting information and actuating decisions. This layer does not only include the hardware per se, but also operating systems and software libraries enabling the programming of such devices. Data are transported from devices to IoT system by a **Network Communication Layer** that defines the physical technology and protocols used to transport the data. Gateways – collecting data from devices and transferring them to other systems - are part of this layer. When equipped with sufficient computing power, gateways can act as edge computing nodes enabling cloud-edge architectures. The **Processing Layer** (that may be located at the edge or in the cloud) enables the remote device management and the edge analysing of data streams. The **Storage Layer** offers efficient solutions (centralised or decentralised) to store historical data for long term analysis and processing. The **Abstraction Layer** provides a unified interface to access data covering both data semantic (i.e. describing the meaning of the data) and access protocol (i.e. the way you can access and query data). In this layer often information from single sensors (e.g. temperature) and actuators (e.g. thermostat) are used to create higher level models of real world (e.g. a room in a building). On top, the **Service Layer** provides functionalities to enable the development of IoT applications, including service orchestration and advanced analytics. The **Applications Layer** includes tools for advanced visualisation, analytics and

[14] Lin, Shi-Wan, et al. "The industrial internet of things volume G1: reference architecture." *Industrial Internet Consortium* (2017): 10-46.

[15] "Reference Architectural Model Industrie 4.0 (RAMI4.0) - An Introduction" Plattform Industrie 4.0 (2018)

[16] "Reference Architecture for IoT Enabled Smart Cities", D2.10 (2018)

reporting of IoT solutions. The **Collaboration and Processes Layer** enables the integration of IoT platforms with existing enterprise solutions and other external systems.

The non-functional properties idenfied cover different dimentions that are typical of distributed systems, such as: Availability, Dependability, Manageability, Scalabilty, Integrability, Interoperabilty and Composability. Addiotionally, a key property for IoT System is the intelligence: the capacity of the system to derive knowledge and decisions from the different data captured by the IoT system.

2.2 IoT Applications

Nowadays, the range of IoT applications is very wide and covers an always enlarging set of domains. A market analysis of the different domains supported by IoT applications is discussed in Section 3. In here we briefly present some of the most typical scenarios in the most relevant domains:

- **Healthcare**. IoT contributed to the evolution and innovation of the healthcare services. IoT have been successfully adopted to, for example: control drugs/medicines, increase automation in hospital management, individual health in real-time, track pandemies[17]
- **Smart Cities & Communities**. IoT revealed as a key technology to monitor city (from environment to any other aspect, such as parking and waste) and to optimize resources (transports, water, energy, …) and ultimately increase quality of life of citizens. It's ability to provide KPIs and instrument to "measure" the city proved to be as well important in engaging citizens and increasing their awareness of their own city.
- **Smart living**. IoT is contributing to increase the automation of homes, providing better quality of life, energy saving and support for elder people.
- **Industry 4.0**. IoT enabled the machine-to-machine communication across the manufacturing plant, enabling real-time monitoring and control of the manufacturing processes. This ultimately allows to improve the quality of the production and its control leading to novel products and levels of product customisation on the market, while containing costs.
- **Retail**. IoT proved to be a key technology to increase supply chain efficiencies, develop new services, and reshape the customer experiences. Typical applications include: tracking goods, real-time inventory, information exchange among suppliers and retailers, and automated delivery capabilities.
- **Transports**. Self-driving cars are becoming a reality thanks to IoT: different sensors are collecting the status of the car, and by leveraging on external data sources (e.g. real time traffic, maps, …), able to advice drivers, and to drive autonomously the vehicle.
- **Energy**. Thanks to IoT, it is possible to montor the behaviours of electricity suppliers and consumers and, hence, improve the energy efficiency.
- **Smart Food & Farming**. IoT is becoming an important instruments in agri and farming industry. The ability to measure in real time different aspects of crops and animal farms, allows for optmisation and automation of different processes such as watering, harvesting, and animal feeding.

2.3 Key enablers for a Next Generation Internet of Things

The European landscape, as detailed in Section , is very active on evolving Internet of Things and related technologies and the European Commission, seen it as central, supports a wide set of research a policies related to the area, including the Next Generation Internet initiative. A critical challenge for

[17] See in Annex II the literature discussion on IoT and COVID-19.

the upcoming years is the need to 'leverage EU technological strength to develop the next generation of IoT devices and systems' taking full advantage of the key enabling technologies of 5G, cyber-security, distributed computing, Artificial Intelligence (AI), Augmented Reality and tactile internet in order to build a sustainable and competitive European ecosystem in IoT area to ensure 'end-user trust, adequate security and privacy by design' covering all the relevant aspects of interoperability, including architectures, devices and tactile/contextual[18].

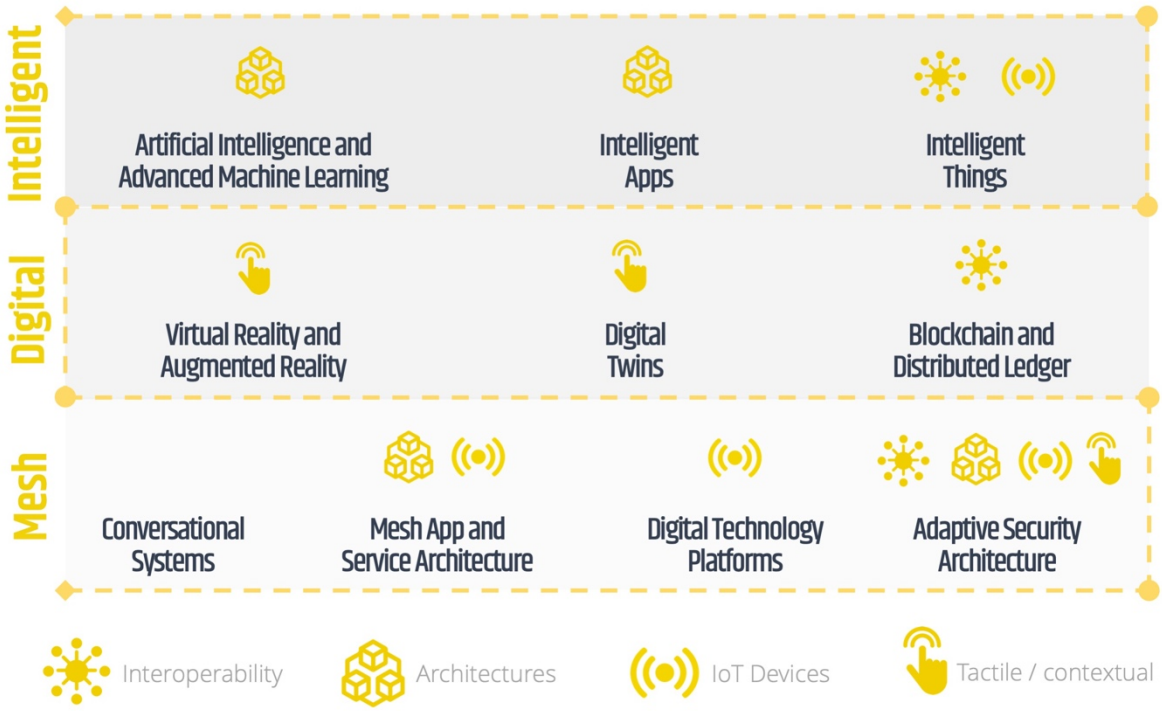


Figure 3. European Research, Innovation and Implementation related to Internet of Things

In this context, key enablers for a Next Generation Internet of Things have been identified in the following technologies:

- **Edge Computing** : increasingly, over the last few years, different scenarios show the limitations of a pure cloud-centric approach to service delivery platforms. For different reasons (e.g. latency, privacy, reliability), platforms and solutions enabling the processing of data at the edge of the network (where the data is generated) are arising on the market, although challenges are still to be solved in relation to edge computing. It is no mystery that several IoT scenarios are pushing and demanding for the adoption of Edge Computing (also in combination with distributed ledgers, making data computation distributed, and data governance decentralised). The ability of taking decisions 'locally' and in reliable way (i.e. regardless of connectivity with the cloud), is the main driver for the adoption of edge computing within IoT solutions. Clearly Edge Computing is not only an enabler for IoT but also for other technologies where computation at the edge enables novel capacities and application scenarios. Compared to other adoption scenarios, IoT may have specific requirements that edge computing needs to support.

[18] EC. ICT work programme 2018-2020 (2018)

- **5G**: cheap, reliable and scalable internet connectivity is a key requirement for several IoT scenarios. 5G, the new evolution of mobile internet technologies spanning from radio access to backbone management, aims to tackle requirements posed by IoT large deployments beyond what today is possible with LPWAN and other technologies. Beyond that, 5G introduces novel means to deliver virtual infrastructures and explores novel mechanisms to virtualise traditional hardware resources. The virtualisation of mobile infrastructure will fuse connectivity and edge computing infrastructures. These infrastructure-related innovations have a key importance for IoT, opening up new ways to deliver and manage IoT infrastructures. Europe is playing a major role on 5G R&D, thus exploiting its positioning to influence the future of IoT infrastructures, which is a key opportunity for Europe to gain global leadership.
- **Artificial Intelligence and analytics**: albeit Artificial Intelligence has been around for many years, the recent evolutions in terms of AI software platforms and hardware platforms and the availability of massive data sets to test and apply AI combined with increasing computing capability (e.g., HPC, etc.), enabled its wide adoption in several real-life scenarios. This new wave of Artificial Intelligence research and application has a fundamental importance for Internet of Things, by enabling extraction of unexpected 'intelligence' from sensed data, the automatic actuation based on 'intelligent' models (e.g. self-driving cars), the higher automation in the management of a plethora of devices and their generated data. More importantly, Artificial Intelligence, in several scenarios, can be applied today at the edge, enabling the usage of AI algorithms close to the devices. The adoption of AI in IoT requires AI to be supported at the edge and not only in the core cloud: performing AI algorithms efficiently at the edge demands for low power computing devices specialised in support of AI algorithms.
- **Augmented Reality and Tactile Internet**: IoT can act as a broker between the assets of the physical environment and the digital infrastructures, while AR serves and supports the digital interaction in real time with the physical environment. The combination of these two technologies has, and still is leading to new possibilities, experiences and applications in all the domains where extreme or difficult conditions from real life (low visibility, accessibility, remote locations, high temperature, etc.) must be faced and overcome. Thus, adding the AI dimension to IoT expands enormously its possibilities in all verticals. It is widely considered that IoT platforms will move rapidly and with big steps to the next level with the emerging 'Tactile Internet and the intelligence at the edge, creating interactive, conversational IoT platforms with new user interfaces to engage with things and humans'[19], adding the human-centred perspective and sensing/actuating capabilities in the human-objects-systems interaction[20]. Of course, the key enablers for this to happen are powerful devices and high-performance networks.
- **Digital Twin:** more than a technology, the digital twin is a concept that relies on the combination of different technologies (IoT, artificial intelligence, machine learning and software analytics) to realise the digital replica of a living or non-living physical entity. The aim of this approach is the ability to monitor, control and simulate in the most realistic way a physical system. The approach is largely advocated in the manufacturing and healthcare sectors and brings new challenges to the understanding of the relation between the digital

[19] AIOTI, Research and Innovation Priorities for IoT, 2018.

[20] Petar Popovski, "The Supernatural Touch of Tactile Internet, Big Data, AI, and Blockchain", 2018.

world (as sensed by IoT devices) and the physical world (humans included). Such relation in the digital twin concept often explores the 'human' side of the interaction between humans and machines, aiming to understand how humans perceive and interact with the technologies.

- **Distributed Ledgers:** most of the platforms dominating today's IoT market relies on centralised data management. The advent of distributed ledgers, following the hype of bitcoin derived technologies, advocates for novel approaches for data management. These approaches enable for a decentralised governance, where all the actors in the ecosystem play a role in the validation and acceptance of the data entering the ecosystem, and data owners can have direct control over who in the network can access their data. In the context of the Internet of Things, both the ability to ensure truthfulness of the data and authorising data access in a distributed way are interesting concepts. In some sectors, these technologies are becoming enablers for new scenarios around trusted data (e.g. food provenance). Despite some promising results in some IoT related scenarios, it is also true that distributed ledgers showed limited applicability in other scenarios, where for example real-time requirement is strict.

3 ECONOMIC OPPORTUNITY FOR EUROPE AROUND IOT

NGIOT as part of T3.1 activities developed the "Market Research and Business Modelling" with the objective to provide an indepth analysis of the IoT market, IoT application domains, IoT-related emerging business models and technology enablers to help identify economic opportunities and challenges related to the research, development and implementation of IoT-related activities. The focus of the report is to align with the priorities and industry-needs, in order to serve as an input for the NGIOT Roadmap to enhance Europe competitiveness in the global market for IoT products.This section summarizes the "Market Research and Business Modelling" report and available as Annex I.

3.1 Market dimensions and segmentation

Studies from the different selected sources present a very positive projection with significant growth in the upcoming years for the IoT market (Hardware, Software and Services). Reports from IHS Markit[21], Ericsson[22] and IoT-Analytics[23] show an estimated number of global connected devices ranging from 7 to 9 billion in 2017, with projected growth from 15% to 30% Compounded Annual Growth Rate (CAGR) depending on the industry, the geography and the type of connection. Variations across projections are due to different metrics and methodologies used to calculate the market potential.

The studies also rank the importance of IoT in different domains, highlighting Industrial IoT and Smart Cities as the most important domains, followed by healthcare, smart home, energy, transportation and agriculture. Despite the differences in the projections and importance of each domain, two important insights can be noted: the most important domains for IoT are similar across every study, the number of connected devices is growing rapidly across all the studying domains.

As for market value, projections from Bain[24], EY[25] and IoT analytics[26] based their global IoT expenditure numbers ranging from USD$1.1 Trillion to USD$1.5 Trillion by 2025, with CAGRs that stay in the range of 13.6% to 22%. Geographically, these projections position Asia-Pacific (APAC) as the biggest region in terms of volume, followed by North America and then Europe, the Middle East and Africa (EMEA). However, all of them point out EMEA as the region with the highest relative growth.

[21] HIS Markit. 8 in 2018: The top transformative technologies to watch this year (2018)

[22] Ericsson. Ericsson Mobility Report (2018)

[23] IoT Analytics. State of the IoT 2018 (2018)

[24] Bain & Company. Unlocking Opportunities in the Internet of Things (2018)

[25] FICCI. Future of IoT (2019)

[26] IoT Analytics. State of the IoT 2018 (2018)

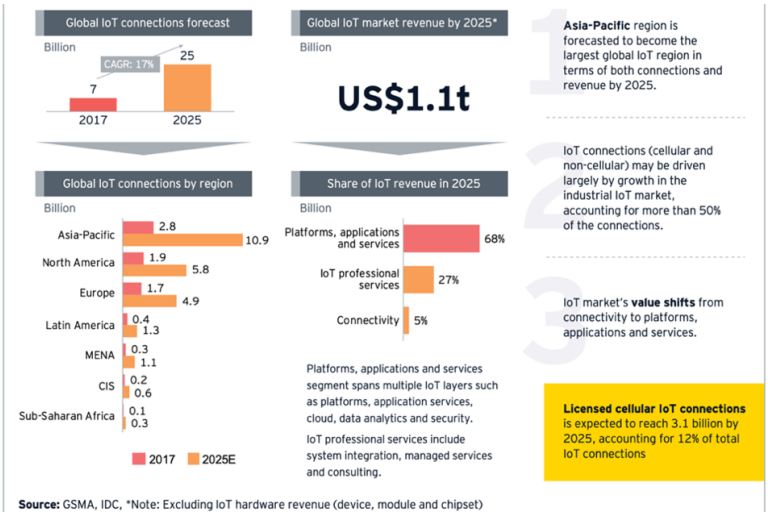


Figure 4. Market value forecast by region[27]

In order to draw conclusions of the most pressing challenges and opportunities for Europe, the market analysis aims to look at the impact of IoT across three dimensions: Industry Domains, Technology Enablers and Business Models. After defining what these dimensions entail, the European Context section digs deeper into how the dimensions interact in the region in order to derive the Opportunities and Challenges.

3.1.1 IoT Industry Domains

On a survey elaborated by KPMG, with over 750 tech leaders ranging from Fortune 500 executives to start-up entrepreneurs, respondents align towards pointing that IoT will drive the greatest business transformation across many industries in the next three years, bringing benefits to life, society and the environment[28]. Because of the breadth of reach of IoT, the study selects the following industry domains of interest, basing the selection on the initial market analysis of the NGIOT scoping paper.

- **Energy Management:** everything related to power generation and distribution.
- **Manufacturing:** from efficiency gains to optimization of supply chains.
- **Transportation:** covers the logistics issues from industrial to commercial transportation.
- **Smart Cities & Communities:** solutions for better governance and collective life quality.
- **Smart living:** home automation through connected smart appliances.
- **Healthcare:** from wearables to specific healthcare applications.
- **Smart Food & Farming:** from food production to processing and distribution.
- **Retail:** everything related to the last linkage of the traditional value chain, the end-customer.
- **Media:** Advertising and customer-targeting.
- **Insurance and Finance:** any kind of risk assessment and protection.
- **Safety and Defence:** from emergency response to better monitoring.

[27] FICCI. Future of IoT (2019)

[28] KPMG. The Changing Landscape of Disruptive Technologies (2018)

3.1.2 IoT Value Chain

Due to its nature, which allows the use and re-use of data, the IoT value chain becomes non-linear and it is difficult to represent it in a single dimension. However, to understand how value is created in an IoT context, Figure 5 shows a simplified IoT value chain. This diagram reflects the overarching nature of IoT and how it can be applied in the different industry domains. It also helps understanding the role that technology enablers play by influencing the different links (e.g. Edge/Cloud computing in the Connectivity link).

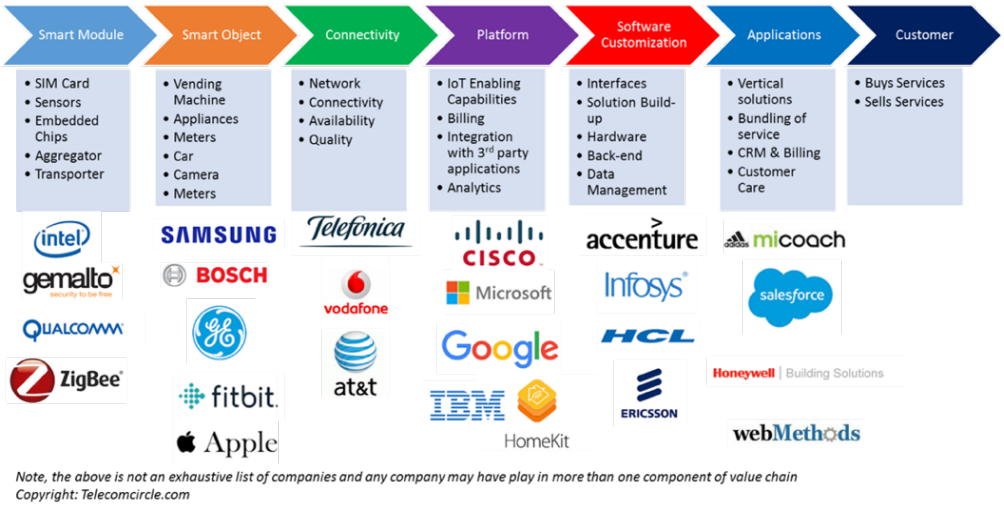


Figure 5. IoT Value Chain[29]

3.1.3 Market perspectives on Key enablers for a Next Generation Internet of Things

Because IoT solutions entail more than enhanced sensing/actuating capabilities, the market analysis takes a look into the following key enablers identified for IoT (cf. Section 2.3), with aim to understand how they may impact the IoT market.

- **Edge and Cloud computing**: Surging as complementary paradigms of data processing and storage, these drivers of IoT balance the location of computational power and storage at the edge of the network and through the internet. The increasing IoT requirements of real time data collection, process, analysis and actuation drive the development of optimal edge computing solutions. Gartner estimates that driven by IoT, data processing outside of the data centres will pass from 10% to over 75%[30]. Some of the worldwide initiatives and players:
  - Cloud: Amazon AWS, Google Cloud, Microsoft Azure and IBM Cloud are the biggest cloud providers worldwide[31], followed by Alibaba Cloud which plays the biggest role in China, whereas in Europe the landscape is more fragmented.
  - Edge: as a fragmented and relatively young industry, the biggest players come from cloud providers and other knowledgeable companies. With Microsoft notably holding over 300 patents[32], Amazon (Greengrass, FreeRTOS, Lambda@Edge), DELL CME, HPE, IBM Edge Computing and Cisco Edge and many other smaller companies play an

[29] Telecom Circle. Internet of Things – Business Models (2016)

[30] Gartner. What Edge Computing Means for Infrastructure and Operations Leaders (2018)

[31] Gartner. Gartner Says Worldwide IaaS Public Cloud Services Market Grew 31.3% in 2018 (2018)

[32] ZDNET. Ten edge computing vendors to watch (2018)

important role. Edgeir provides an extensive company list[33] with some big, medium and small players worldwide.

- **5G/6G**: This technology enabler refers to the new generation of mobile communication that supports a massive number of devices with a diverse range of speed, bandwidth and quality of service. The fifth generation of mobile cellular technologies encompasses reliability, latency, scalability, security and ubiquitous mobility. The 5G Observatory divides the service in 3 big scenarios according to the application needs[34], Enhanced Mobile Broadband (EMBB), massive Machine Type Communications (MMTC) and Ultra Reliable Low Latency Communications (URLLC). MMTC promises to allow cheap, reliable and scalable internet connectivity, which is a key requirement for several IoT scenarios. With its augmented spectrum, 5G aims to tackle requirements posed by IoT large deployments beyond what today is possible with Low Power Wide Area Networks (LPWAN), achieving massive and critical communications with a complete vision deployed by 2021[35]. Some of the worldwide initiatives and players:
  - Besides the 5G providers, McKinsey identified 3 main players poised to win: component suppliers, industrial automation companies and manufacturers[36]. In terms of providers, the clear global players are Ericsson, Nokia and Huawei. As for the component suppliers, the providers vary withi EMBB, URLLC and MMTC, with Qualcomm, Skyworks, Intel, Broadcom and Xilinx[37] as some of the top firms.
- **Artificial Intelligence**: Blended with IoT, AI offers augmented intelligence in the data analysis process. The availability of massive data sets to train, test and apply AI (Big Data) [38] combined with increasing High-Performance Computing (HPC[39]) capability enabled its wide adoption in several real-life scenarios. This combination is expected to kick off the next wave of performance improvements, especially in the industrial sector[40], by enabling extraction of unexpected 'intelligence' from sensed data, the automatic actuation based on 'intelligent' models (e.g. self-driving cars), the higher automation in the management of a plethora of devices and their generated data. Also, as Artificial Intelligence becomes a reality across several application[41], its combination with IoT is moving towards the edge[42], enabling usage of algorithms closer to the devices. In fact, a study on Emerging Technologies in Electronic Compnents and Systems [43] identifies AI at the edge as one of the key opportunites for Europe.

[33] EDGE IR. Edge Computing Companies (2020)

[34] GSMA. Internet of Things in the 5G Era (2019)

[35] NOKIA. 5G for Future Industrial Internet (2019)

[36] Mc Kinsey. The 5G era (2020)

[37] CNBC. Here are the 5 biggest beneficiaries of the 5G rollout: Jim Cramer (2019)

[38] Novarica. Big Data, IoT, and AI Maturity Levels (2017)

[39] insideHPC. AI-HPC is Happening Now (2018)

[40] Mc Kinsey. Smartening up with Artificial Intelligence (AI) (2017)

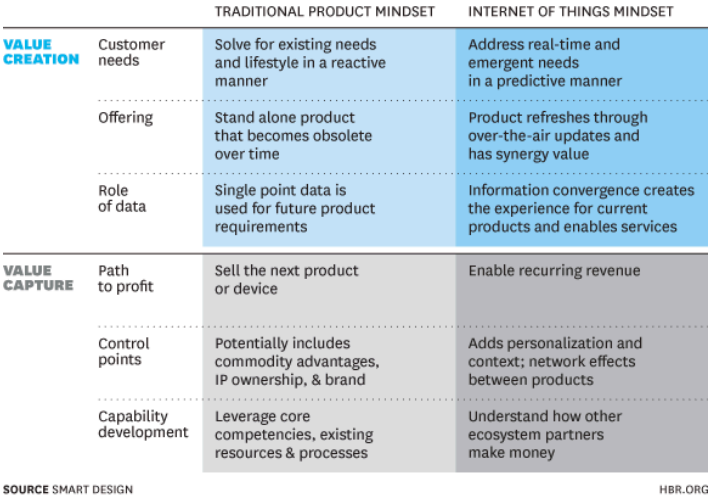
[41] Novarica. Big Data, IoT, and AI Maturity Levels (2017)

[42] I-Scoop. Building management evolutions and drivers in the age of IP and IoT (2020)

[43] DECISION Etudes & Conseil. Study on Emerging Technologies in Electronic Components and Systems (ECS) – Opportunities ahead (2020)

3.1.4 IoT Business Models

Recent development in the IoT enables hybrid solutions that merge physical products and digital services possible[44], creating a new array of totally new business model patterns. Some of these are new business models, while others are not entirely new but are rather traditional models enhanced by the new capabilities of technology and the shift in the mindset driven by these capabilities, as shown in Figure 6.



		TRADITIONAL PRODUCT MINDSET	INTERNET OF THINGS MINDSET
VALUE CREATION	Customer needs	Solve for existing needs and lifestyle in a reactive manner	Address real-time and emergent needs in a predictive manner
	Offering	Stand alone product that becomes obsolete over time	Product refreshes through over-the-air updates and has synergy value
	Role of data	Single point data is used for future product requirements	Information convergence creates the experience for current products and enables services
VALUE CAPTURE	Path to profit	Sell the next product or device	Enable recurring revenue
	Control points	Potentially includes commodity advantages, IP ownership, & brand	Adds personalization and context; network effects between products
	Capability development	Leverage core competencies, existing resources & processes	Understand how other ecosystem partners make money

SOURCE SMART DESIGN HBR.ORG

Figure 6. IoT mindset shift[45]

Some of the explored innovative IoT-related Business Models are:

- **Subscription Model:** a service or asset provided for a specific amount of time in return for a fee. (e.g. similar to leasing schemes). Easily adjusted and understandable by customers.
    - **IoT-as-a-Service:** whole or part of the solution offered for a fee. KONE, for example, uses IoT to provide preventive maintenance and avoid downtime.
- **Asset Sharing Model:** maximization of asset utilization through sharing, billed based on time or usage
- **The Razor-Blade Model:** IoT product to sell another product. Example: Amazon Dash Buttons.
- **Monetize IoT Data Model:** sale of data and data insights to help decision making. IBM's Watson IoT platform offers insights on the collected data by developing AI solutions to help decision-making
- **Pay-Per-Usage:** charge the customer according to the active time or outcome of a service or a product. IoT enables the application of this model in industries where it was not possible before.
    - **Monetize M2M data buckets:** on demand charges based on data consumption. Pay-per-usage based on data buckets.
    - **Outcome-Based Model:** customers pay for the outcome the product provides. Brother, for example, offers printer leasing by invoicing the printed pages only.

3.2 European Context

EU work programmes so far organised IoT related activities around 3 main pillars, **thriving IoT ecosystem**, a **human-centric approach** and a **single market for IoT.**

[44] Elgar Fleisch et al. Business Models and the Internet of Things (2014)

[45] Harward Business Review. How the Internet of Things Changes Business Models (2014)

It is also important to point out Europe's leading position in smart cities and communities, acknowledging the success of the Large-Scale Pilots (LSP) programme in IoT under Horizon 2020. Further details on European Policies directing the IoT landscape can be found in the next chapter. As for the market report, the objective is to consider the macro analysis of the environment through a PESTLE analysis, and an analysis of European competitiveness under the most pressing industry domains and technology enablers.

IoT will have also a key role in the upcoming work programme part of the Multifinancial Framework 2021-2027 and related to technology development and adoption: Horizon Europe (€80 billion) (Research & Innovation) and Digital Europe Program (€9.2 billion) and Connecting Europe Facility 2 (€3 billion) (Deployment).

3.2.1 PESTLE Analysis

Table 1. PESTLE Analisis.

Political	• European Commission solidity • Brexit could potentially hit the Digital Single Market Initiative • Data privacy and protection is a priority amongst European citizens
Economical	• Europe has the highest growth potential for IoT. • Multiplier effect of Big Data. • Likely trade surplus, using M2M connections as a proxy • Shift in labour skills • High cost of large-scale implementation among other barriers
Societal	• Lack of transparency and scepticism towards technology • Concerns about personal security • Shortfall of digital knowledge and skills • Equal access for consumers and SMEs
Technological	• Lack of low-cost connecting services – smartphone/internet penetration • High costs of Big Data tools and AI development • Edge still not mature – no reference frame from ECCE, fragmented market
Legal	• Competition Law on big data management • Personal Data Protection - GDPR • Standardisation • International flow of data • Missing regulation for specific verticals
Environmental	• Better mapping and decision making regarding renewable energy • Efficiency improves resource and energy management

3.2.2 European competitiveness

With the pressing insights from the global landscape, it is now important to understand where Europe stands in the different domains cited before and how these domains will be influenced by IoT. For that

matter, the matrix of Kearney in Figure 7 shows a picture of where Europe stands in comparison to other regions. This matrix also points to the most influenced industries, making the upper quadrants the industries of focus. The upper right corner shows the industries Europe should prioritize to remain competitive. The upper left corner shows areas where a new strategy can create big opportunities for Europe.

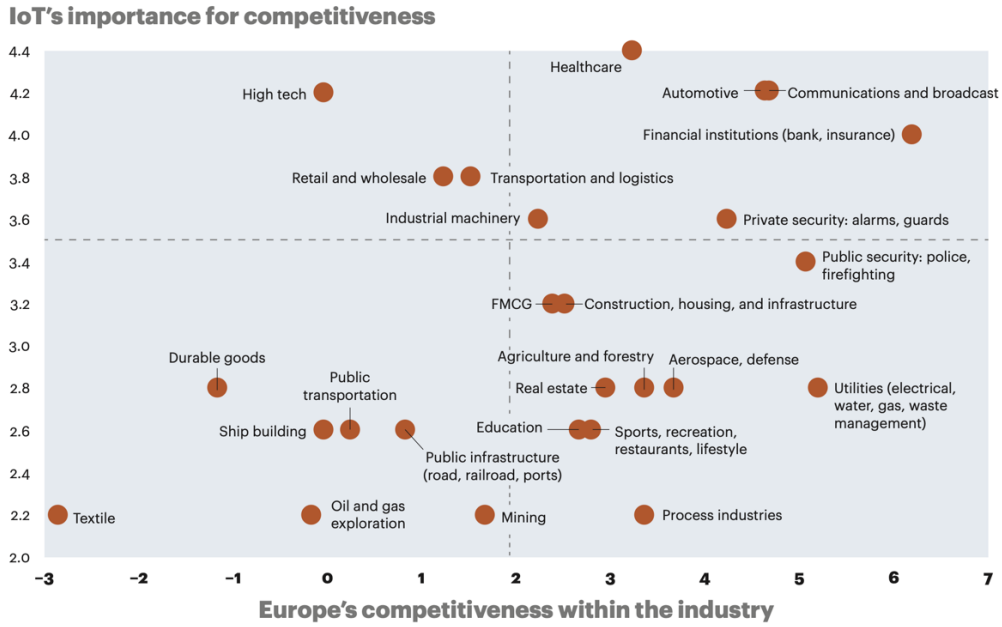


Figure 7. European competitiveness vs. IoT importance[46]

3.2.3 Context by industry domains

Based on Figure 7 and the Scoping Paper, the following industry analyses were prioritized for the first draft:

- **Smart Cities & Communities:** Europe is one of the leaders in terms of smart cities and communities, with over 12 of the top 25 cities of the IESE cities in motion index[47]. This leading position responds to Europe's early efforts to overcome the challenges of developing smart cities and communities through several initiatives aligned with the Europe 2020 targets. By promoting policies and programmes aimed at developing smart cities in a coordinated way[48] and solving funding needs by Private Public Partnerships[49], the EU has managed to quickly develop their "Lighthouse" cities and aims to have over 300 smart cities by 2020[50]. Despite the target seems to not have been reached in the context of the Lighthouse initiative[51], today, Europe counts with various programs constantly reinforcing its Smart City development, from

[46] AT Kearney. The Internet of Things: a new Path to European prosperity (2016)

[47] IESE Insight. New York, London and Paris Firmly Established as the Smartest Cities (2018)

[48] European Parlament. Mapping Smart Cities in the EU (2014)

[49] Osborne Clarke. Smart Cites in Europe (2015)

[50] Energy Post. Europe aims to have 300 smart cities by end of next year (2018)

[51] The web site of the lighthouse projects report around 100 cities: https://smartcities-infosystem.eu/scc-lighthouse-projects

the success of the SynchroniCity LSP project[52] to the centralization and clusters of European Innovation Partnership on Smart Cities and Communities (EIP-SCC)[53].

- **Manufacturing:** Having invested at higher levels than their competitors in other regions, Europe leads the way in Industrial IoT, moving to scale faster with three times more implementations than in the US[54]. Looking at individual countries, Germany paves the way with the automotive and manufacturing sectors leading the adoption rate, driven by mid-market companies[55]. In Gartner's study[56], Software AG outstands as a visionary IoT platform headquartered in Germany, amongst other global players. Followed by the UK, France, Italy and the Nordic and Eastern European markets, the trend is passing from leveraging Industrial IoT to developing new services and solutions, to generating efficiencies and ensure cost savings. Across Europe , IoT related activities and even strategic alliances are implemented like ADAMOS to accelerate the development[57]. Although Europe leads the way in this domain, security, privacy and issues of trust remain important points of attention as they hinder widespread adoption. Bain also estimates that mastering these areas will give European IoT providers a substantial competitive advantage[54]. Another important challenge for this domain lies on the high-tech industry side, where several studies from Kearney show that Europe's high-tech industry is declining[58]. Europe is struggling to keep up with the rhythm of Asia and North America. The world's biggest technology companies nowadays, like Amazon, Google, Baidu and Tencent, are all originated outside of Europe.
- **Healthcare:** Europe faces the trend of ageing population more than ever[59]. Although the region keeps a strong position in this industry, it is not so easy to see how the different players are embracing change. For this industry this is crucial, since, as shown in Figure 8, Healthcare is an industry where IoT is vital for competitiveness. As one of the clusters of global challenges and European industrial competitiveness, healthcare is a top priority, with areas of intervention going from tools, technologies and digital solutions, to personalised medicine and medical systems improvements[60].

[52] SynchroniCity. A guide to SynchroniCity (2020)

[53] EIP-SCC. European Context (2020)

[54] Bain & company. Europeans Extend Their Lead in the Industrial Internet of Things (2018)

[55] CBI. The European market potential for integrated internet of things and big data services (2020)

[56] Garnter. Magic Quadrant for Industrial IoT Platforms (2019)

[57] Smart Industry. IoT Readiness: Is Europe up to it? (2018)

[58] Kearney. Rebooting Europe's high-tech industry (2013)

[59] LSP. The European Large-Scale Pilots Programme - Driving IoT Innovation at Scale in Europe (2019)

[60] EC. Horizon Europe: the next EU research & innovation investment programme (2021 – 2027) (2019)

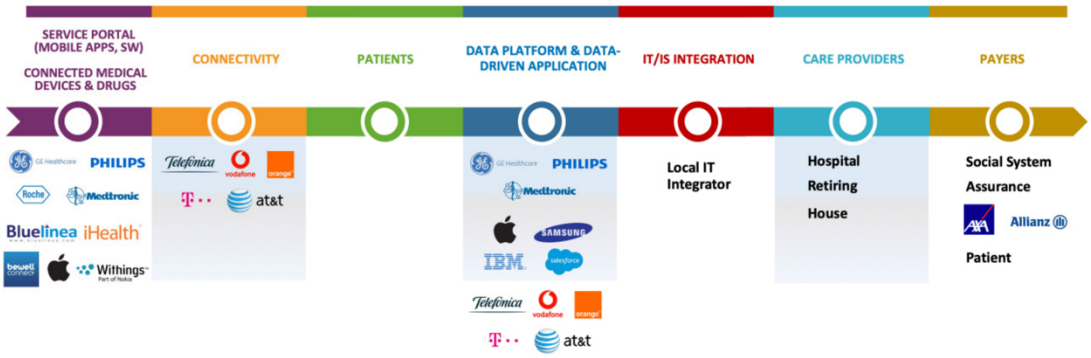


Figure 8. Healthcare Solutions Value Chain

- **Transportation:** With its strong mobility industry, Europe stands as an important voice when it comes to smart transportation. Starting with solutions like Asset & Fleet management and Freight monitoring in the ground transportation sectors, to Airport optimization and Passenger traffic flow, the transportation sector is an area where Europe is leading the way[61]. In the Transport sharing area, Europe also stands out with numerous bike sharing, car sharing and other services across different cities. Lastly, many European cities have already integrated smart solutions in their public transportation systems, significantly improving the quality of this service.
- **Agriculture & Smart Farming:** Although agriculture does not rank in one of the upper quadrants in Figure 7, it remains an important vertical for IoT in Europe. From the LSP IoF2020, Europe has fostered the creation of a symbiotic ecosystem to bring together the supply and demand sides of IoT technologies and the Agri-food sector[62], making it the first industrial sector to create a framework focused on data sharing[63]. This framework, based on an EU code of conduct on agricultural data sharing, helps generate trust and the necessary tools to create a competitive advantage at a regional level. Furthermore, the European Agricultural Machinery Association rolled out its strategy, establishing some guidelines and best practices in the industry[64].

[61] IDC. Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination (2014)

[62] https://www.iof2020.eu/about/impact

[63] AIOTI. IoT data marketplaces for the agri-food sector: a first look to use cases for smart farming and across the food chain (2020)

[64] CEMA. Full deployment of agricultural machinery data-sharing: technical challenges & solutions (2020)

3.2.4 Context by enabling technologies

Based on the Scoping Paper and enabling technologies analysis the following technologies were prioritized for the first version:

- **Edge and Cloud Computing:** Because of the types of edge computing and the slight differences in the definitions, some of the market analyses report that more than 60% of the companies in Europe use Edge to a certain extent[65]. It is interesting to note, however, that in a Deloitte study with over 2000 executives[66] only 6% signalled Edge Computing as an impactful technology, whereas 64% said Cloud infrastructure would have a profound impact. IDC's European report states that European companies are lagging 2 years behind the U.S. companies who lead the edge computing development[67].

  IDC estimates that although Edge is a marginal part of IoT infrastructure spending, it will grow rapidly, to reach 25% of total spending by 2022, with big manufacturing and automotive companies leading the way. The Electronic Components and Systems (ECS) agenda created by AENEAS, Artemis-IA and EPoSS puts the development of AI at the edge for IoT solutions on the spot, as a strategic opportunity for Europe thanks to its alignment with Europe's requirements of safety and privacy, and its expertise in embedded systems[68]. Amongst the upcoming initiatives, the Edge Computing Consortium Europe (ECCE) stands out, with over 18 companies cooperating to specify a reference architecture, develop reference technology stacks, identify best gaps and recommend best practices[69].

  In terms of landscape, Ericsson defines a value stack for Edge where companies addressed each of the layers, including Services, App Development, App deployment and enablement, Software, Hardware, Connectivity and Site[70]. Within these layers, 4 main types of companies stand out: Hyperscale cloud providers (AWS, Microsoft Azure, Google and Alicloud), System Integrators (JR Automation, Wood, etc.[71]), Operations Technology (Siemens, Bosch, Schneider Electric, etc.) and Technology Vendors in each layer individually (Software, Hardware, Services). Although these 4 categories present similarities, their focus varies from company to company. However, a trend of lock-in strategy can be observer amongst the hyperscale cloud providers, who leverage on their cloud solutions to provide an end-to-end solution, integrating all the layers[72].

- **5G/6G:** Europe is playing a major role in 5G, thus exploiting its positioning to influence the future of IoT infrastructures, which is a key opportunity for Europe to gain global leadership. It is calculated that in 2019 around 45% of the Smart City projects were done in the European Union, spending in 5G research and standards that drive areas like IoT and Machine-to-Machine (M2M) communication[73]. Europe has also the input from projects across several

[65] I-Scoop. Edge computing: the what, how and where of the edge (2020)

[66] Deloitte. The fourt Industrial Revolution (2020)

[67] IDC. The Technology Impacts of Edge Computing in Europe (2019)

[68] AENEAS, ARTEMIS-IA and EPoSS. ECS Strategic Research Agenda 2020 (2020)

[69] EETimes. European Consortium to Develop Standard Edge Computing Platform (2019)

[70] Ericsson. Edge computing and deployment strategies for communication service providers (2020)

[71] Control Engineering. 2020 System Integrator Giants (2020)

[72] STL Partners. AWS, Azure & Google at the edge: How much 27 fit is telco edge computing? (2017)

[73] Reporter Link. Europe 5G in IoT Market to 2027 - Regional Analysis and Forecasts by Radio Technology; Device Range; End-User Industry (2019)

vertical domains where it has been determined that in most cases, the specifications of 5G fulfill the requirements for successful implementation of solutions across the Smart Mobility, Smart City, Smart Energy, Smart Agriculture, Smart Manufacturing and Smart Health verticals[74]. Furthermore, cybersecurity and privacy remain two of the main concerns for Europe in this area[75].

- **Artificial Intelligence:** The White Paper from the EC signals the landscape of AI in Europe[76], describing Europe's current position of strength in digital competencies, research centres, innovative start-ups, and world-leading robotics and manufacturing with AI solutions. It also highlights Europe's potential and gives recommendations to leverage on these strengths, which promise to drive the complementarities of AI and IoT. Within these recommendations, focusing on SMEs and start-ups is also pointed out on a Roland Berger study, indicating that AI start-ups in the IoT area are weekly underrepresented in comparison with other regions[77]. As this combination has the potential to change business models, European businesses have to further embrace the opportunity to think strategically about AI and IoT instead of following shorter term goals[78].

3.3 Economical and societal challenges linked to IoT in Europe

This chapter builds on the NGIOT scoping paper[79], presenting an overview of the most important challenges in the IoT domain from an economic and policy perspective:

- **Support for SMEs and start-ups (E1)**: SME enterprises in Europe are the core financial driver of growth[80], thus Europe needs to ensure their smooth transition towards innovative solutions, including IoT technologies. The adoption of IoT may bring a lot of added value to companies and it may give them a certain competitive advantage. Companies which will not be able to adopt IoT appropriately might suffer and later also disappear from the market. Small players often face the problem of capital barriers to enter the market as well as lack of recognition and trust, as they cannot use a strong and well-established brand (e.g. like Amazon, Google etc.). IoT4Industry signals 5 main barriers: lack of competences, regulation, unknown benefits, transparency, and mindset[81].

  Additionally, it is crucial to support start-ups (e.g. providing access to business angels, investors, VC funds, accelerators, supporting partnerships with big players within that industry), as start-ups have the capacity to disrupt the market and to push innovation into new sectors in agile ways. However, it is not easy to find attractive IoT start-ups. Most of IoT start-ups fail to show a substantial recurring revenue stream, their revenue is often based on project-based consulting fees or through the support of one-time proof of concept (PoC) implementations rather than highly scalable software[82]. Supporting SMEs and start-ups can be

[74] AIOTI. IoT Relation and Impact on 5G (2019)

[75] Open Access Government. The cybersecurity challenges of 5G and IoT (2020)

[76] EC. The European AI Landscape (2018)

[77] Roland Berger. Artificial Intelligence – A strategy for European startups (2018)

[78] DIGITAL SME. DIGITAL SME input on the EC's White Paper on Artificial Intelligence (AI) (2020)

[79] NGIOT. Building a roadmap for the Next Generation Internet. Research, innovation and implementation 2021 – 2027 (2019)

[80] Selamat et al. Big Data and IoT Opportunities for Small and Medium-Sized Enterprises (SMEs) (2019)

[81] IoT4Industry. SME Barriers and opportunities for adopting IoT (2018)

[82] IoT Analystics. IoT Investments 2018 (2018)

rather difficult because of this, but it is still the best alternative for Europe to limit market monopolisation by the major and well-established players and at the same time strengthen European innovation in IoT domains.

- **Accurate economic parameters estimate (E2)**: Currently, it is very challenging to estimate the key parameters used by investors in their decision-making process. Investors are interested in the return on investment estimate (ROI), revenues, costs, profits and risk profiles of investments in IoT. Vodafone identifies that different treatments of IoT technologies across EU's specific industry policies (Cellular vs. Non-Cellular solutions) significantly distort investment choices and hinder Europe's innovation and adoption of IoT[83]. In this regard, looking at trends and past investments in innovative technology solutions could provide guidance. IoTUK also proposes a comprehensive toolkit for investments evaluation[84].
- **Data and information as critical assets (E3):** The key value of the data gathered from IoT devices is not the data itself, but the information which can be extracted from the data. In order to price data, it is necessary to have a better understanding of data management, interoperability and standards, services provided around the data (security, protection, etc.), data ownership and accountability, ethics, and how they can influence the future value of data. In addition, questions to take into account include the potential connectivity partners have to monetise the data, the size of the market, market accessibility, market entry barriers, and competing data providers and services.
- **Increase of digital skills and competencies (E4):** The implementation of IoT will require a significant number of skilled workers in IT, computer science, big data science, artificial intelligence and other related technologies. This requires not only the development of study programmes at bachelor, master and PhD levels, but also on a professional basis to regularly update employees and professionals already in the work process through tailored courses, workshops, interactive trainings, etc. An important target group is children and adolescents - children should be educated about technology from primary school and supported to choose a career in technology-related domains, removing current gender gap barriers.
- **Build Trust (E5):** Building trust among current and potential IoT users, policy makers and citizens is essential for the successful adoption of IoT. The technology adoption curve could be an inspiration, including learning from early adopters, building trust on both supply and demand side and changing mind-sets to support technology implementation. Other initiatives aiming at building trust may include raising awareness through success stories and building trust through transparent guidelines and frameworks that address the ethical and privacy implications of IoT. Educating people on the value data can bring to their everyday lives and helping to achieve sustainability goals are also important steps towards improving trust with regards to IoT implementation. However, the key questions are how to make individuals and enterprises trust IoT technologies sufficiently to change their habits and processes for the better; and how to prepare organizations for the inclusion of IoT technologies? Behaviour change requires the right attitude, which makes it a complex goal.
- **Identification of the Key Regulatory and Legal Issues (E6):** New technologies entail legal and regulatory issues. The most important regulatory and legal issues and open questions related to IoT should be identified and gaps and controversial open questions need to be solved in a transparent and agile way. A point that should be highlighted is the speed of the new regulations. Having the regulations at the right time is very important for optimal exploitation

[83] Vodafone. A new IoT regulátory framework for Europe (2019)

[84] Future Cities Catapult. IoT investment case toolkit: smart parking (2016)

of IoT; otherwise, investors will be reluctant to invest in new IoT-related technologies and businesses, as they may face a serious risk of their investment objective not being approved.

- **Interoperability and Replicability (E7):** IoT technologies will generate huge amounts of data. Data can only attain its true value when it can be shared and monetised across domains, frameworks, shareholders and countries. For that reason, common harmonised data models should be adopted. Following harmonised data models, harmonised functionality should be focused on. An example could be the harmonised implementation of some open source components, in particular the FIWARE context broker that is specifically enabling the vision towards a system-of-systems approach to facilitate interoperability and expansion. Another example is the Open & Agile Smart Cities network which connects 140 smart cities in 29 countries globally and strives to establish the Minimal Interoperability Mechanisms (MIMs) that are needed to create a market for smart cities and IoT. MIMs are simple and transparent mechanisms, ready to use in any city, regardless of size or capacity. By implementing MIMs, cities increase the speed and openness of innovation and development, whilst decreasing cost and inefficiency. MIMs allow cities to engage in global digital transformation, addressing the lack of convergence of standards. IoT solutions must be interoperable and replicable, which requires orchestration of business processes, effective collaboration and practices. This might require more technologies than just data and information interoperability (e.g. TM Forum develops services and technology agnostic operational management APIs and testing capabilities). The effective integration of cross-domain data in business and organizational processes is another aspect.
- **Security and Reliability by Design (E8):** In order to work on the above points, we must ensure the security and reliability of the technology solutions. At the time of scaling and increasing the workload, it is of utmost importance to ensure that the solutions remain reliable, especially in terms of privacy and cybersecurity.
- **Innovation procurement (E9):** Ensure that public procurement is well aligned with the dynamics of IoT and the consequent changes in the IoT applications. The emphasis must be put on the cooperation of public administrations in Europe with the aim to encourage first movers and estimate appropriately associated risks. As a benchmark, successful procurement strategies from the past can be used. However, the current public procurement has a clear preference towards long-standing companies and does not support the 'try before you buy' model. A key element is to develop trusted KPIs and certification schemes, linked to broader initiatives such as DESI-local and the UN SDGs.
- **Sustainability (E10):** Ensure sustainability related to the increasing number of new technologies, materials for sensors, electronics and power source. Not only in environmental terms, but also social and economic terms for the long-term strategy to be viable.
- **Cohesion (E11):** Focus on bridging the smaller and rural communities and developing areas also, not just the innovation and economy frontrunner territories. There are interesting business opportunities in developing countries.
- **Sovereignty (E12):** Ensure Internet sovereignty, as IoT is based on the Internet. Although data sovereignty could be solved by data centres in Europe, there is a significant dependency on non-European cloud infrastructure and data are also handled by non-European service providers.

3.4 Opportunities linked to IoT in Europe

The untapped potential of IoT can be found on a wide range of areas, going from the effective allocation of resources to the empowerment of citizens in Europe. For this reason, the following opportunities are listed as general opportunities first, followed by industry specific.

3.4.1 General and technology driven opportunities

- **Standardisation in IoT:** Taking into account the estimated growth of the IoT ecosystem and the growing need for interoperability of IoT solutions, standardization will play more and more an important role. Until now firms have been building their own strategies and solutions with a wide range of platforms and technologies and therefore one of the consequences is the fragmentation of the technological solutions which may also result in a fragmentation of the market. Standards represent an essential part of the organization and functioning of modern society including ICT and information security. In the case of IoT technologies one of the consequences of an unstandardized IoT is that many devices are not "plug and play" ready. In many cases end-users must download software and drivers to make them work with existing technologies. If one of the goals, also for the Digital Single Market, is to facilitate the spreading of and access to technology there is a need to make it easier to use. Standards can play an important role in this context by promoting best practices, integration and interoperability of systems, privacy and security requirements.
- **The creation of value and the IoT trust framework:** In order to facilitate the growth and development of the IoT market and of the value chain a fundamental element is the adoption of a "trust by design" approach. We have already seen in the section devoted to societal challenges why the security and the protection of privacy needs to be build in askey features in IoT deployments. As regulation is fragmented along national lines (e.g. GDPR is implemented with slight differences across Europe), different stakeholders have taken an initiative for the creation of an IoT trust framework to raise the level of security of IoT devices and related services. The framework developed covers different areas focusing on the following principles: authentication, encryption, security, updates, privacy, disclosures, control, communications. The framework identifies core requirements that manufactures, service providers, distributor/purchasers and policy makers need to understand and embrace to develop a trust framework for the IoT[85].
- **IoT and the Digital Single Market:** IoT deployments and devices represent a building block of the digitisation of our society and economy, a context into which people and objects are interconnected through communication and networks. The Digital Single Market Strategy adopted in 2015 already included elements for consideration of a European approach to the IoT. The strategy adopted by the European Commission underlines the need to avoid fragmentation and foster interoperability. The document published in 2016 "Advancing the Internet of Things in Europe" has specified the EU vision based on three pillars: 1) a thriving IoT ecosystem; 2) a human-centred IoT approach; 3) a single market for IoT. All these pillars, and their strengthening have a market relevance both internal and external for the EU. The pillars need to be bases on a sustainable ecosystem development, the promotions of common standards and the need to look at societal challenges posed by IoT developments. The "European data economy" will need to propose solutions that facilitate the free flow of data among European countries and rules concerning liability issues in complex environments in order to enhance legal certainty and trust in complex environments such as the IoT one. According to the European Commission the value of the data economy will increase to EUR 643 billion by 2020 representing 3,17% of the overall EU GDP.
- **5G and IoT:** The transition of many companies and organizations towards adoption of IoT will also be grounded in the adoption of other key technologies such as the fifth generation of wireless technologies (5G). 5G offers to corporates important benefits in terms of data speed, latency, reliability, efficiency, capacity and security. 5G is therefore expected to support a wide array of new solutions. As highlighted by KPMG: "Some of the benefits of IoT could be realized

[85] Internet Society. IoT Trust by Design (2018)

within an existing telecommunications infrastructure, but previous wireless technology generations do not have the capability to integrate with autonomous robots or advanced technologies. In contrast, when IoT is combined with 5G networks in a transformation strategy, the goals of i4.0 come within reach"[86]. The deployment of 5G will therefore constitute a building block of the Digital Single Market and the European Union has already taken several initiatives already from 2013 by establishing a Public Private Partnership on 5G (5G PPP) and by funding several research projects. 5G standards are also one of the five priority areas under the European industry initiative. The 5G Action Plan for Europe was adopted in 2016 with the goal of starting the deployment of 5G services in all the EU Member States by the end of 2020. Given the market relevance of 5G deployments the European Commission launched also the European 5G Observatory in 2018 to monitor major market developments in a global context. For the development of proper market solutions, the role of Member States has to be taken into account as well, for this purpose a report on national strategies and their consideration under a European perspective has been published. 5G deployments are to be considered in a market perspective also from a security and geopolitical, for this reason a coordinated risk assessment was undertaken.

- **Open Innovation role:** A fruitful interaction between IoT growth and the role of open innovation could bring new opportunities and innovations to companies and to society. Open Innovation, like the one advocated by IoT, brings in a more distributed and connected approach. In fact, with its reliance on open source/open data/ open standards it changes the proprietary paradigm of research and development that characterizes many companies. Open Innovation contributes to companies looking beyond their boundaries to seek and utilize inflows and outflows of knowledge. To this extent the value created through data collection and data analytics by IoT deployments can be one on of the most important tool of a new approach. Because of the importance of SMEs for the EU, academic research recommends that Open Innovation policies must move outside of the walls of large companies, fostering an open innovation environment that is equally beneficial to SMEs[87]. However, policies should take into account the multiple challenges that SMEs face while implementing open innovation, which lead to uncertainty and even renunciation of open project participation[88].

3.4.2 Domain specific opportunities

- **Agriculture and Smart Farming:** IoT technologies enable drop control, remote monitoring of livestock, data collection about soil, crop and cattle conditions and it reduces human intervention (and thus labor costs) in favour of automated farming. Also, data analysis helps optimize farming and hence save costs and/or increase revenues.
- **Healthcare:** the introduction of IoT in healthcare supports hand hygiene monitoring systems, remote health monitoring through wearable devices and smart medical apparatus manufacturing. The combination of smart sensors and cloud computing is used to optimise the flow of patients, staff, equipment and medical supplies hospital wide. This gives many opportunities for extension of revenue streams in the healthcare industry. Due to optimization based on dynamic data, it can reduce inefficiencies and enable better allocation of financial resources. Biometric wearables to track health and lifestyle provide important information

[86] KPMG. Converging 5G and IoT: a faster path to smart manufacturing (2019)

[87] Chesbrough Henry and Vanhaverbeke Wim. Open Innovation and Public Policy in the EU with Implications for SMEs (2018).

[88] Ullrich A. and Vladova G. Weighing the Pros and Cons of Engaging in Open Innovation. Technology Innovation Management Review, 6(4): 34-40 (2016).

concerning the tailored medical treatment as well as solid data for health insurance companies.

- **Energy Management:** IoT technology can be employed to create smart grids that price and route power, based on the demand and prevent blackouts. This leads to optimization of resources and better service.
- **Manufacturing:** IoT can be used in manufacturing for predictive maintenance of machinery based on the sensor data collected. These further leads production line monitoring with sensors to optimise equipment utilisation. IoT implementation would also help manufacturers increase business profitability and productivity of both humans and machines, by streamlining production processes and automating plant machinery with RFID chips that store product configuration data, work instructions & work history. Predictive analytics engine help to make the future manufacturing plants more autonomous in terms of predicting and fixing potential disruptive issues, which might lead to significant losses.
- **Media:** IoT supports hyper-personalised advertising to drive relevancy and effective targeting, hardware sensors can measure and analyse metrics such as high footfall timings, popular store sections and products, whilst also targeting consumers with push marketing messages based on their individual purchasing habits. This can remarkably increase sales, while the cost of the implementation of IoT technology is relatively low. This boost profits.
- **Insurance and Finance:** The implementation of IoT across several domains and continuous data collection and evaluation leads to new models of risk assessment (including a user's credit & claims history, and the size and type of property owned etc.). The risk models are highly personalised and data-led and data from several connected devices are analysed (wearables, smart home appliances and connected cars used by the policyholder etc.). This helps insurers to monitor the policyholder's personal habits and behavioural preferences and develop better models effectively assessing the insured risk and offering added value. Yet, this brings major challenges in terms of ethics and privacy.
- **Transportation:** Predictive maintenance, traffic jams predictions, optimal route calculation and car tracking are one of the ways of utilization of IoT in transportation which lead to cost saving. Mobility as a service stands as a tremendous opportunity to create value in the public transport field[89].
- **Smart cities and communities:** One of the domains, where IoT has an enormous potential. Monitoring and managing traffic and transportation systems, power plants, water supply networks, waste management, buildings, community services and others provides a solid basis for analysis and predictions, thus enabling cost optimization and effective allocation of resources.

[89] IDC. Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination (2014)

4 THE EUROPEAN ECOSYSTEM AROUND IOT RESEARCH, INNOVATION AND DEPLOYMENT

4.1 From IoT to the Next Generation IoT: the EU vision

In line with the Digital Single Market Strategy[90] and its pillar 'maximising the growth potential of digital economy', the European Commission launched the Digitising European Industry (DEI) initiative[91] in 2016 with the aim of reinforcing the EU's competitiveness in digital technologies and supporting their integration in all economic sectors.

As outlined by the European Commission, the Internet of Things (IoT) represents the next step of disruptive digital innovation where 'any physical and virtual object can be connected to other objects and to the Internet, creating a fabric of connectivity between things and between humans and things'.[92] The Internet of Things is a technology enabler that is central to the successful implementation of the EU Digital Single Market Strategy. Similarly to cloud computing, big data, artificial intelligence, robotics, machine learning, IoT will contribute to profoundly transforming the EU's economy and society.

Even though the Internet offers enormous opportunities for our society, it also brings along significant risks for our society. To address the risks while creating better opportunities, Europe aims to re-invent the next generation of the Internet by 'shaping a value-centric, human and inclusive Internet for all.'[93]

To this end, in autumn 2016, the European Commission launched the Next Generation Internet (NGI) initiative with the ambition to contribute to creating a 'highly adaptive and resilient', 'trustworthy' and 'sustainably open' human-centric Internet. The NGI aims to shape the development of the Internet of tomorrow into an Internet of humans that responds to people's fundamental needs, including trust, security and inclusion, and reflects the values and norms that we enjoy in Europe[94].

Through an ambitious research and innovation programme with an EC investment of more than € 250m between 2018 and 2020, NGI's focus is on advanced technologies including, in addition to IoT, privacy and trust, search and discovery, decentralised architectures, blockchain, social media, interactive technologies, as well as technologies supporting multilingualism and accessibility.

This plethora of digital technologies is key to unleash the potential of digital transformation and relies very much on the capability to build, manage and support a 'network of everything' ensuring availability and reliability of the whole IoT infrastructure. Improved end-to-end reliability and availability demands for increased performance of devices, networks and platforms. Such improvements can be achieved thanks to innovative solutions coming from research on Artificial Intelligence, cloud computing, ultra-reliable connectivity beyond 5G, edge computing, and big data. Towards this vision, both the networks and service delivery infrastructures are key, grouping the set of concepts, technologies and solutions that are needed to design and engineer the next generation Internet of Things.

This vision is supported by the current ICT H2020 Programme that identifies, as a critical challenge for the upcoming years, the need to 'leverage EU technological strength to develop the next generation of IoT devices and systems' taking full advantage of the key enabling technologies of 5G, cyber-security,

[90] EC. A Digital Single Market Strategy for Europe (2015)

[91] EC. Digitising European Industry - Reaping the full benefits of a Digital Single Market (2016)

[92] EC. Advancing the Internet of Things in Europe (2016)

[93] NGI. NGI, For an Internet of Humans (2019)

[94] Michiel Leenaars et al. Next Generation Internet 2025 (2018)

distributed computing, Artificial Intelligence (AI), Augmented Reality and tactile internet in order to build a sustainable and competitive European ecosystem in IoT area to ensure 'end-user trust, adequate security and privacy by design' covering all the relevant aspects of interoperability, including architectures, devices and tactile/contextual[95].

With the mission-oriented Horizon Europe and Digital Europe vision, complemented by structural funds and private investments, Europe has laid out the tracks to tackle this complexity, to the benefit for European citizens, and beyond. As the new Commission was announced, the focus on digital and the link to the digital single market was further emphasised, including Commissioner-designate Executive Vice President Margrethe Vestager given the portfolio title "a Europe fit for the Digital Age. This marks not only a level of ambition but also a strategic integrated approach to technology, market creation and competition not seen before.

The Internet of Things (IoT) is a technology enabler that is central to the successful implementation of the EU Digital Single Market Strategy. Similarly to cloud computing, big data, Artificial Intelligence, robotics, machine learning and 5G, IoT will contribute to profoundly transforming the EU economy and society.

To facilitate and accelerate the uptake of IoT across all economic sectors, the EU strategy for IoT is articulated around three pillars: a thriving IoT ecosystem, a human-centred IoT approach and a single market for IoT.

A significant breakthrough was made in March 2015 when the European Commission together with IoT industry players set up the Alliance for the Internet of Things[96] (AIOTI) to coordinate ongoing activities and build a consensus on how to unleash the full potential of IoT in Europe.

In 2016, the IoT-European Platforms Initiative[97] was formed to promote the idea of open and easily accessible platforms and to build a vibrant and sustainable IoT-ecosystem in Europe.

Given the strategic importance of IoT, a dedicated Focus Area was introduced into the Horizon 2020 ICT Work Programme for 2016-2017 and major efforts have been undertaken 'to enable the emergence of IoT ecosystems supported by open technologies and platforms.'[98]

In the same year, the IoT Large-Scale Pilots (LSPs) Programme[99] was launched to test and foster the deployment of IoT solutions in Europe in five specific domain areas: smart living, smart farming & food security, smart cities & communities, wearables, and autonomous driving. Three further Large-Scale Pilots started in 2019 to tackle the issues of energy, agriculture, and digital transformation in health and care.

In parallel, the European Commission decided, in 2018, to support a further set of eight projects specifically addressing security and privacy issues, as rebuilding trust in technology and equipment is essential to ensure the roll-out and large uptake of IoT solutions in Europe.

Altogether, the EU is investing almost EUR 500 million[100] in IoT-related research, innovation and deployment under Horizon 2020 for the period 2014-2020. All those concrete actions aim to better prepare Europe for the challenges ahead and support its capacity to act independently and defend its

[95] EC. ICT work programme 2018-2020 (2018)

[96] https://aioti.eu/

[97] https://iot-epi.eu/

[98] EC. Cross-cutting activities work programme 2016-2017 (2016)

[99] LSP. The European Large-Scale Pilots Programme - Driving IoT Innovation at Scale in Europe (2019)

[100] https://ec.europa.eu/digital-single-market/en/research-innovation-iot

sovereignty in the Digital Age. As outlined in a recent Strategic Note[101], digital technologies and the global race for technological R&I leadership will play a pivotal role in ensuring Europe's strategic autonomy.

Moreover, further concrete steps have been taken to translate the EU NGI Vision into key EU documents: for instance, the Horizon 2020 ICT Work Programme 2018-2020[102] and one of its four Focus Areas 'Digitising and transforming European industry and services' (i.e. the Digitisation Focus Area). 'The Digitisation Focus Area will support digitisation in an integrated way, making sure that European industries and businesses are well positioned to make the most of the opportunities offered by the digital age.'[103]

As discussed in the following sections, the works on the 2021-2027 Multiannual Financial Framework (MFF) introduced new visions and strategies complementing the Digital Single Market strategy of the previous MFF.

4.1.1 The new policy context

The European Commission (EC) is currently setting priorities for the next Multiannual Financial Framework (MFF) of the European Union which will span the 2021-2027 period. Under the leadership of Ursula von der Leyen, the upcoming MFF developed by the new EC will play a strategic role in supporting the EU strategic priorities such as:

- **A European Green Deal**, with the goal of "becoming the world's first climate-neutral continent by 2050 is the greatest challenge and opportunity of our times".
- **An economy that works for people**, under the ideal that "The EU's unique social market economy allows economies to grow and to reduce poverty and inequality. With Europe on a stable footing, the economy can fully respond to the needs of the EU's citizens."
- **A Europe fit for the digital age**, by empowering people with a new generation of technologies and sustaining the Digital Single Market Strategy to create better and larger opportunities for European companies
- **Protecting our European way of life**, promoting a "vision for a Union of equality, tolerance and social fairness".
- **A stronger Europe in the world**, to reinforce European role as responsible global leader working to ensure the highest standards of climate, environmental and labour protection.
- **A new push for European democracy** to ensure a stronger role of European citizens in the decision making process and in the setting of European priorities.

In line with the above political guidelines, EC is defining and releasing a whole new set of strategies. On 19th February 2020 Ursula von der Leyen announced[104]:

"Today we are presenting our ambition to shape Europe's digital future. It covers everything from cybersecurity to critical infrastructures, digital education to skills, democracy to media. I want that digital Europe reflects the best of Europe – open, fair, diverse, democratic, and confident."

[101] EPSC. Rethinking strategic autonomy in the digital age (2019)

[102] EC. ICT work programme 2018-2020 (2018)

[103] EC. Digitisation Research and Innovation - Transforming European Industry and Services (2017)

[104] EC. Shaping the Europe's digital future (2020)

Shaping Europe's digital future[105], provides the overall strategic plan to implement through different actions the "Europe fit for the digital age" political guideline. This strategy pushes three key objectives to promote technological solutions that will help Europe pursue its own way towards a digital transformation that works for the benefit of people and respects our fundamental values:

1) Technology that works for people;
2) A fair and competitive economy; and
3) An open, democratic and sustainable society.

These objectives will be pursued by a number of key actions, some of which have been already started or announced:

- **A European strategy for data**[106] through which the "EU can become a leading role model for a society empowered by data to make better decisions – in business and the public sector". To this aim, the strategy pushes the creation of a single market for data within Europe supported by a ***High Impact Project on European data spaces and federated cloud infrastructures***.
- **An Industrial Strategy package** focusing on EU industry transition toward climate neutrality and digital leadership as way to promote EU global leadership. The package includes different documents, most relevant ones for cloud and digital services are:
  - **A new Industrial Strategy for Europe**[107]: setting the lines for an industrial strategy aligned with core European societal and market values, including the investments on sustainable digital infrastructure needed to ensure EU digital sovereignty.
  - **An SME Strategy for a sustainable and digital Europe**[108]: focusing on concrete actions to support SMEs (as the heart of EU industry) toward a sustainable digital transition.
- **A White Paper on Artificial Intelligence**[109], promoting a European approach to artificial intelligence putting upfront key European values such as excellence and trust.
- A new set of policies[110] to ensure the sustainability of the EU economy linked to the **Green Deal**. In these landscape, one of the key goal is to "make data centres and ICT infrastructures climate-neutral by 2030".
- **A new agenda for the European strategic autonomy**[111] that encompasses the changes brought by the digital technologies and underlines the need for Europe to support its capacity to act independently and defend its sovereignty in the Digital Age;

[105] EC. Communication: Shaping the Europe's digital future (2020)

[106] EC. Communication: A European strategy for data (2020)

[107] EC. A new Industrial Strategy for Europe (2020)

[108] EC. An SME Strategy for a sustainable and digital Europe (2020)

[109] EC. White Paper on Artificial Intelligence: a European approach to excellence and trust (2020)

[110] EC. Supporting the green transition (2020)

[111] EC. Rethinking Strategic Autonomy in the Digital Age (2020)

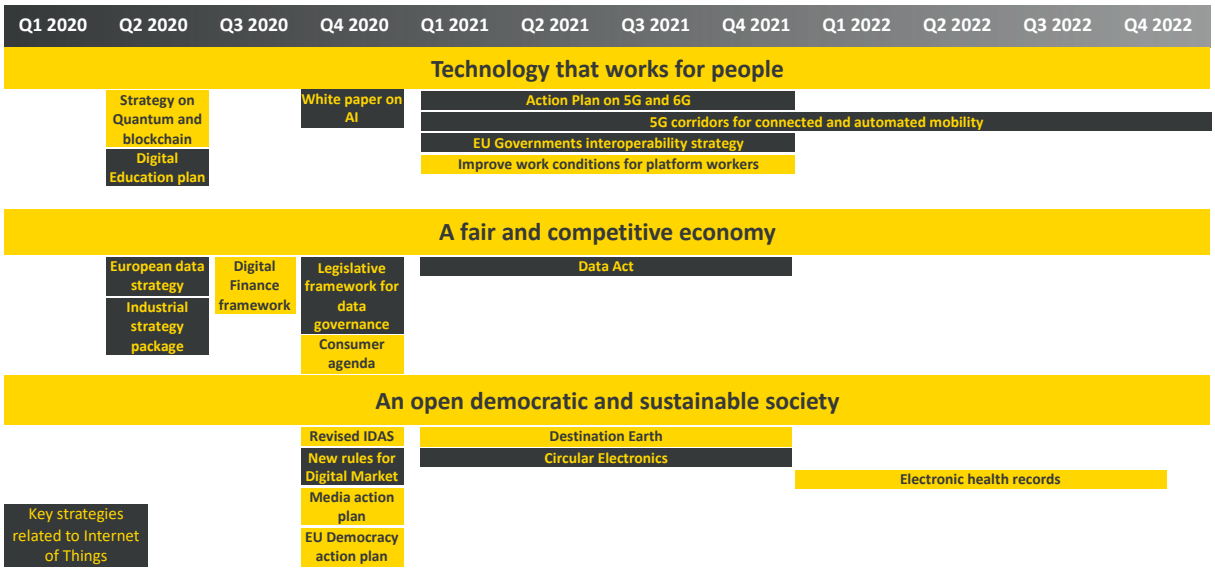


Figure 9. EC strategies release timeline and relevance to Internet Things

Within the Digital Single Market Strategy, the Internet of Things (IoT) represents the next step of disruptive digital innovation where 'any physical and virtual object can be connected to other objects and to the Internet, creating a fabric of connectivity between things and between humans and things.' The Internet of Things, in combination with cloud and edge computing, artificial intelligence, and 5G will contribute to profoundly transforming the EU economy and society. In many sector, IoT related technologies will act as main drivers of the digital transformation, thus the High Impact Project on European data spaces and federated cloud infrastructures and related initiatives are foreseen to integrate as well Internet of Things and build on top of it. In particular, the following data spaces – covered by the European data strategy – are supposed to include data generated from IoT devices or platforms: Industrial, Green Deal, Mobility, Health, Energy and Agriculture.

"Europe must lead the transition to a healthy planet and a new digital world", as stated by Ursula von der Leyen. The European Commission committed to achieve climate neutrality by 2050 as part of the strategy towards achieving the SDGs by 2030. Following the announcement on the European Green Deal, Europe committed to key actions such as energy decarbonisation, circular economy, and sustainable land use and food systems and to sustaining them by investing in education, promoting innovation, and harnessing the potential of digital technologies for Europe's sustainable development. IoT and other digital technologies will play a fundamental role in shaping a sustainable Europe.

4.1.2 Future work programmes

As part of the new MFF 2021-2027, the European Commission is currently working on three key pillars to support the digital transformation in Europe:

- Horizon Europe, the new research and innovation programme to succeed Horizon 2020 with a proposed € 100 billion budget, including € 15 billion on the 'Digital, Industry and Space' cluster.
- Digital Europe, a brand new programme focusing on building the strategic digital capacities of the EU and on facilitating the wide deployment of digital technologies, with a proposed € 9.2 billion budget.
- Connecting Europe Facility 2, the follow-up of the current CEF programme, focusing on the creation of transnational digital infrastructures with a proposed € 3 billion budget.

These three programmes are meant to complement each other and will play a key role in Europe's digitalisation in connection with the Internet of Things technologies. While Horizon Europe will provide future outlook by supporting cutting edge research and innovation, Digital Europe and Connecting

Europe Facility will foster the market deployment of mature technologies (including those that proved maturity and business viability from Horizon 2020 and, in future, Horizon Europe). The introduction of the Digital Europe programme may play a key role in supporting the deployment of mature research and innovation outcomes, bridging them between the Research and Market penetration phases, thus helping to overcome the so-called "Valley of Death".

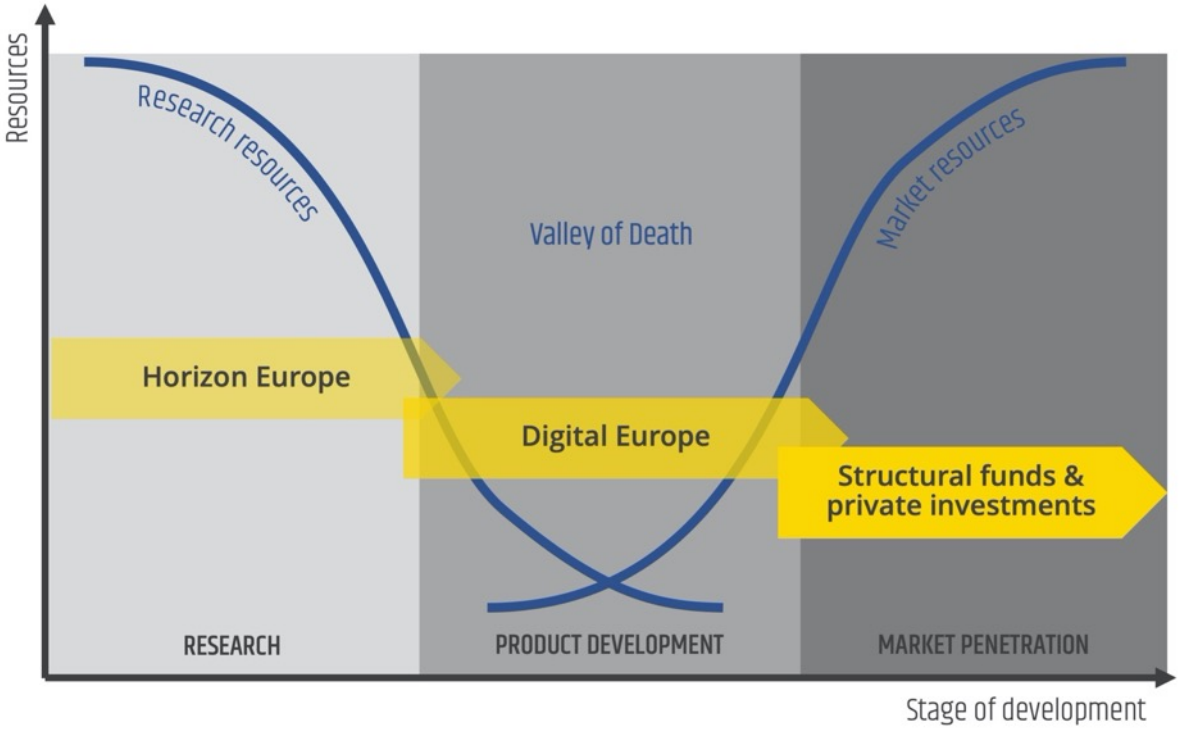


Figure 10. From research to market: the role of EU instruments.

4.2 Ecosystem

Different actors are taking a key role in Europe to support development and take up of IoT. In this section we don't aim at providing a full picture (which is covered in the stakeholders analysis in D4.2), we provide few higlights taking into consideration the contributions to IoT technologies outlook.

- **Initiatives.** In the current European landscape, several initiatives drive IoT or supports its development. Primary actors in the driving ecosystem include AIOTI[112] and IoT Forum[113]. Other actors focus on linked technologies, these include for example: NGI[114] focusing on human centric internet, 5G-IA[115] focusing on next generation mobile networks and services and BDVA[116] focusing on data-centric technologies to generate value from data insights. Other

[112] https://aioti.eu/

[113] https://iotforum.org/

[114] https://ngi.eu

[115] https://5g-ia.eu/

[116] http://www.bdva.eu

initiatives again focus on specific application area, such as: OASC[117] focusing on reference solution for smart cities and ARTEMIS[118] focusing on embedded intelligent systems industry.

- **Industries.** The European industrial ecosystem linked to IoT in Europe is quite wide, spanning from embedded device developer, network operators, system integrators, platform providers and vertical solution providers. Several of these players have a clear (and public) vision of the role of IoT and related technologies into shaping our future society. ATOS in its "Look Out 2020+ Tech Trends"[119] classify Internet of Things together with Deep Learning, Digital Twin and Autonomous Vehicles as Transformation technologies. SAP in its "Innovation Guide"[120] identifies a number of key scenarios where IoT, in combination with other technologies, will revolutionate the market or - in some cases – it is already transforming it.
- **R&I projects.** In the past few years a number of project have been active in relation to IoT as part of the Internet of Things unit or other units part of DG Connect. In the recent past, the LSP (Large Scale Pilot) projects and IoT-EPI (IoT-European Platforms Initiative) projects collected the most relevant projects aiming at developing and piloting IoT technologies. In 2019 a new set of Pilot have been kicked off as part of the Digital Platform cluster of projects part of the Technologies and Systems for Digitising Industry unit.
- **SDOs.** Standard development organisations are one of the primary actors in the establishment of IoT interoperable solutions. Within Europe, the most promitent actor is clearly ETSI that contributed to a number of IoT related initiatives, including the SmartM2M and OneM2M families of standards, the Low Throughtput Networks and Ultra Low Energy standards for IoT communication.
- **Open Source communities.** IoT since its infance have been linked with Open Source. Nowadays a number of mature project, spanning from hardware to platform and scenario specific soluitions are getting mature. Some of these communities, such as Arduino[121] for the hardware, and FIWARE[122] for the platforms, have deep European roots.

[117] https://oascities.org/

[118] https://artemis-ia.eu/

[119] https://atos.net/content/mini-sites/look-out-2020/tech-trends/

[120] https://innovation-guide.sap.com/?technologies=IoT

[121] https://www.arduino.cc/

[122] http://fiware.org/

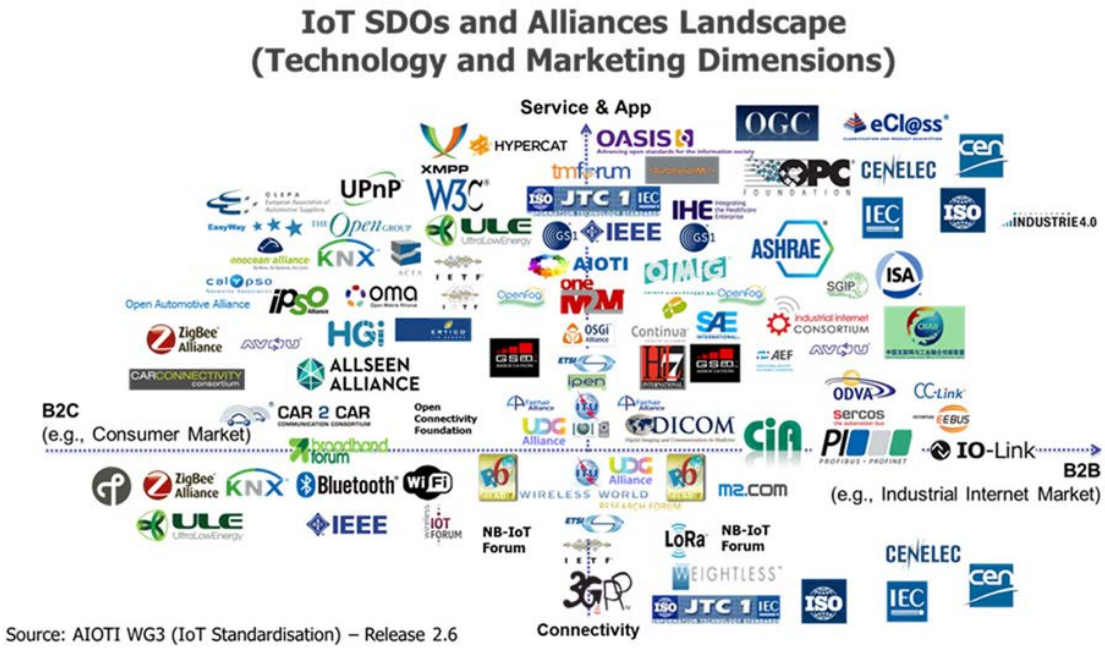


Figure 11. IoT SDOs and Alliances Landspace (source AIOTI WG3)

4.3 Map of European initiatives

As reported in the **IoT Large Scale Pilot (LSP)** Programme eBook[123], IoT brought the Internet society to the next stage of development, with new values introduced, piloted and established, along with new IoT-oriented business models and building on a combination of connected devices, infrastructures, services, information and stakeholders as part of a consistent and integrated ecosystem. These values have been used, tested and assessed through the LSPs strengthening even more the fact that the adoption of IoT is a key step and challenge towards the 'Digitising European Industry' strategy and the Next Generation Internet of Things. In such a configuration, IoT acts as a catalyst for the digital revolution and brings transformation in several societal aspects, although, posing new challenges to the entire ecosystem. LSP projects focused on five key domains: i) Smart Living solutions for ageing people; ii) autonomous driving vehicles and releated mobility services; iii) smart food and farming solutions; iv) innovative services for cultural and heritage industry and v) Smart City services. All the projects focused on common aspects in the respective domain to deliver reference solutions that could be easily replicated across Europe. Between January 2019 and 2020 a new set of Large-Scale Pilots for Digitising European Industry started covering: Agriculture, Energy, Healthcare and Manufacturing.

The **AIOTI** Strategy 2017-2021[124] covers several key aspects related to IoT and related technologies. It highlights how new technological advancements will emerge from current R&D activities on 5G networks, Artificial Intelligence (AI), robotisation, quantum computing, blockchain and nanotechnologies uses. Such advancements will lead to new application domains with IoT-oriented concepts and solutions. The strategy also highlights that the biggest and ***most critical challenge remains the trust in IoT technologies and applications in and by society***. Such a challenge requires discussion around the involvement, education and information of the stakeholders in their context and environment. In 2019 AIOTI released "AIOTI Vision and Recommendations: European IoT challenges and opportunities 2019 – 2024" [125]: a set of reccomendations for the upcoming work programmes. In

[123] LSP. The European Large-Scale Pilots Programme - Driving IoT Innovation at Scale in Europe (2019)

[124] https://aioti.eu/aioti-strategy-2017-2021/

[125] AIOTI. European IoT challenges and opportunities 2019–2024 (2019)

particular the reccomendations highlights: the ***importance of a human-centric approach*** – as the European vision for IoT - ensuring safety, security, privacy and trust; the ***priority of closing the digital divide*** between EU regions and the Member States; the importance for EU society of the development of key ***IoT-enabled solutions addressing societal challenges like energy efficiency, climate-change, carbon-neutral smart cities, security of food supply and healthy water***; the key role - for the creation of the European digital single market - of ***cross-sectoral IoT data marketplaces***; the primary role of cyber-security strategy for safeguarding IoT technology and applications, whilst ensuring privacy by design; the ***advancement of the convergence of IoT with other enabling technologies*** such as next-generation connectivity, AI and edge computing.

Along the same line, the **Road2CPS** Technology and Application Roadmap[126], which focuses on Cyber-Physical Systems, highlights ***the importance of IoT solutions enabling interoperability***. IoT, according to Road2CPS, is ***strongly connected with the advancements in cloud computing, AI, Human Machine Interaction (HMI), Big Data and data analytics***. This report, while it considers IoT as an infrastructure technology, also points out a number of critical challenges towards ***secure and reliable IoT architectures, focusing on interoperability, identification and privacy in IoT devices, the emergence of common data models for domain specific platforms*** and the need for common IoT architectures.

Complementary to this, the Strategic Research and Innovation Agenda (SRIA)[127] published by **BDVA**, considers ***IoT as one of the key drivers of the Big Data phenomenon***, as IoT technology enables the connection of a variety of smart devices or objects that trigger a rapidly growing amount of data. To tackle the challenge of the exponential growth of IoT-generated data, BDVA SRIA highlights that it is fundamental that ***IoT is effectively and efficiently combined with other key technologies like 5G, Cloud, High Performance Computing (HPC), Edge Computing and Big Data*** towards next generation digital infrastructures.

The Future Internet Roadmap for the **FIWARE** ecosystem[128] strengthens both reports and recommendations discussing issues such as the change and advancement that IoT brings to the media domain and the technological challenges that IoT brings to Future Internet, summarising them to ***the growth of a number of connected IoT devices, the management of this infrastructure towards robust and reliable IoT-based services, and the further use of the collected data to create relevant valuable information and knowledge***.

The Strategic Research and Innovation Agenda 2021-27, NetWorld2020/**5G PPP**[129] strongly supports this position by clearly describing how IoT in conjunction with cloud computing can lead towards the emergence of ambient intelligence, a kind of Artificial Intelligence 2.0. Again, the challenges remain from this analysis: ***enable next generation connectivity***, foster built-in network intelligence and provide secure and ***trusted digital infrastructures*** introducing among these challenges also the need for validation of the enabling technologies and especially IoT by means of pilots that involve the future users and the vertical sectors and all these under a reasonable and acceptable security framework.

Focusing more on the security domain, the **European Cyber Security PPP** Strategic Research & Innovation Agenda[130] discusses IoT among other key technologies like embedded 5G, Big Data, quantum computing, cloud, mobile and embedded systems and smart grids as the most relevant and critical towards secure ICT infrastructures. Especially for IoT adoption, the challenges and needs in the cybersecurity domain focus on ***new computational trust models***, the ***inter-connectivity of smart***

[126] Road2CPS. D2.4 - Strategy Roadmap (2016)

[127] BDVA. Strategic Research and Innovation Agenda 4.0 (2017)

[128] https://www.fiware.org/community/fiware-mundus/

[129] Networld 2020. Strategic Research and Innovation Agenda 2.0 (2018)

[130] European Cyber Security Organisation (ECSO). Strategic Research and Innovation Agenda (2016)

systems, the ***interoperability protocols for consistent and efficient communication*** and transfer of information, and the ***trust in IoT devices and IoT frameworks***.

The **AENEAS, ARTEMIS-IA and EPoSS SRA**[131] focuses on Electronic Components & Systems. This SRA, while tackling a wide set of aspects going beyond IoT per se, provides an interesting analysis covering different industrial sectors including transport and mobility, health and well-being, manufacturing, energy and security. Starting from an analsys of challenges in the different industrial sectors, it provides as well challenges for the electronic components and system industry. The SRIA highlights the importance of advancements and adoption of the following technologies: Artificial intelligence and data analytics, Edge computing and novel computing architectures (such as Neuromorphic computing), 5G, Advanced electronics (including Bio-inspired devices and Photonics). A detailed timeframe is provided for the advancement in computing and storage technologies and in process technology for manufacturing of electronic components, which are highly relevant to the IoT edge gateways, devices and sensors development.

Finally, the report provided under the **NGI Initiative**[132] presents a synthesis of research topics related to the societal, economic, design and legislative concerns, and their implications for technological developments of the Internet and among them, the role that IoT has, as one of the key technologies. The report, by identifying clear values and themes, sets the scene for 2021 and onwards for the NGI domain and sets the basis for the emerging discussion on how IoT and Next Generation IoT is positioned towards these transversal topics and key thematic areas towards a human-centric and decentralised internet.

4.4 Global initiatives

IoT centric initiatives are booming worldwide. In North America, **USA**, the world's leading IoT market, launched the SmartAmerica initiative in 2013 as a way to explore IoT potential across different sectors. This leads different initiatives, including US Ignite, a smart city-focused programme, that includes several projects, e.g., the Smart Giga Communities project[133], a network of communities developing a catalogue of reference applications and services to address smart city and IoT challenges.

In Latin America, **Mexico** is aiming at leading the Industry 4.0 market, as declared in the document 'Crafting the Future: A Roadmap for Industry 4.0 In Mexico'[134] released by the Ministry of Economy in 2016. The strategy defined in the document aims at ensuring Mexico's leadership on IoT applications in Latin America and positioning it among the five leading countries in digital solutions and Big Data analysis in 2025.

In Asia, the scene is led by **Japan**, a forefront country on technology innovation. IoT experiments started in Japan in 2010, focusing on large-scale pilot projects on smart grid and smart community. In 2017, through the 'Artificial Intelligence Technology Strategy'[135], Japan switched the priority from the digitalisation of physical infrastructures to the extraction of intelligence from the collected data from physical infrastructures. The focus of the initiative is on three primary areas: productivity, healthcare & welfare, and mobility. Important in the strategy is the investigation of social and biological-related aspects of adopting AI, thus fostering a multidisciplinary approach.

[131] AENEAS, ARTEMIS-IA and EPoSS. ECS Strategic Research Agenda 2020 (2020)

[132] HUB4NGI. NGI Guide v3 (2019)

[133] https://www.us-ignite.org/program/smart-gigabit-communities/

[134] ProMéxico. Crafting the Future: A Roadmap for Industry 4.0 In Mexico (2016)

[135] Strategic Council for AI Technology. Artificial Intelligence Technology Strategy (2017)

Beyond Japan, innovation focused countries such as Singapore and Malaysia are in the implementation phase of their IoT roadmaps. **Singapore** launched in 2014 the Smart Nation initiative[136], to lead the transformation of the country through innovative technologies leveraging the collaboration between public and private actors. In 2019, one of the core projects of the initiative was publicly released: the Smart Nation Sensor Platform[137], a nation-wide platform to integrate sensors to provide services to citizens. Going beyond the Smart City area, in 2017, Singapore's Agency for Science Technology and Research launched the Industrial Internet-of-Things Innovation (I^3) programme[138], focusing on challenges to innovate industry through IoT. Priorities include: Robust data extraction in a harsh and unpredictable environment, Intelligent and secure data processing and transmission at the edge, and Effective data analysis for operational insights.

In **Malaysia**, the National IoT Strategic Roadmap[139], released in 2015, sets the ambitious goal of transforming Malaysia into the Premier Regional IoT Development Hub, focusing on priority application scenarios such as: Connected Healthcare, Traceability of assets, Home & Community Living, and People-friendly Commuting.

Emerging economies, like **India**, are working to keep pace with the rest of the world. Following the release of the "Policy on the Internet of Things" in 2016, India aims to establish 100 smart cities by 2022[140]. The policy stresses the importance of modernizing the agri-food sector through IoT in India, increasing its sustainability. The policy was recently supported by other initiatives, such as the National Digital Communications Policy (NDCP) 2018[141] aiming at innovating the digital infrastructure of the country (from networks to digital platforms and related policies) with the aim of accelerating Industry 4.0 deployment in India.

In Africa, the leading country is **South Africa**, aiming to emerge as the primary IoT actor on the continent, as outlined in the document "National ICT Integrated White Paper"[142] released in 2016. The document, which has a broader scope, covers the challenges the government should take account of in relation to IoT: privacy of consumers and businesses; security for critical devices and systems; incentives to promote fair data sharing; and new regulations to data ownership control and artificial intelligence.

Clearly EU, comporated to global intiatices, is promoting an IoT vision centered around its core value, i.e. putting the end-users at the center of the technologies and ensuring that technologies respect their individual rights. Only South African and Japan give a primary role to such aspects in their programmes. It is also relevant to notice that while in many countries there is a wide set of policy driven initiatives (in same cases policy are the main drivers of IoT solutions as in the case of India, Malaysia and Singapore), as often happens, in the US the action is more driven by large industry, and the governamental support is limited and more oriented toward promotion of best practises rather than active support to development of common technologies and solutions.

---

[136] https://www.smartnation.sg/

[137] https://www.smartnation.sg/what-is-smart-nation/initiatives/Strategic-National-Projects/smart-nation-sensor-platform

[138] https://www.a-star.edu.sg/Research/Research-Focus/Infocomms/IIOT

[139] MESTECC. National Internet of Things (IoT) Strategic Roadmap (2014)

[140] http://smartcities.gov.in

[141] Gov.In. National Digital Communications Policy 2018 (2018)

[142] NSTF. National Integrated Information and Communication Technology (ICT) Policy White Paper (2016)

4.5 Community inputs

4.5.1 Strategy Board

NGIoT has contacted a variety of key stakeholders and initiatives in the field of IoT to co-create an IoT roadmap for research, innovation and deployment. The establishment of a Strategy Board has been crucial in this development, gathering experts in IoT from various backgrounds and representing IoT related alliances, organizations, industry and academia. The NGIoT Strategy Board meets regularly to comment on various working papers produced by the NGIoT consortium, as the scoping paper and the recently published draft IoT roadmap. The Strategy Board works for identifying IoT research trends, gaps and barriers for adopting IoT and to consult on recommendations for the upcoming European and national research and innovation and deployment programmes, identifying priorities and new horizons for the period of 2020-2027. Over the course of two workshops organised in the framework of NGIoT ("Workshop on European Research Support and Contribution to Global Standardisation, Internet of Things Perspectives" and "Workshop on Value Claiming", Switzerland, March 2020), the members brainstormed on measures to maximize the economic and societal impact of European research on IoT for European industry and citizens (see D1.1.)

4.5.2 Thematic Workshops

In addition to the meetings of the NGIoT Strategy Board described above, NGIoT has reached out to a broader community of experts through organising workshops and webinars on specific topics and emerging trends. To achieve a larger impact and mobilise the ecosystem, the workshops have been organised in conjunction with already existing networks and events and in collaboration wth other key players. The NGIoT Strategy Board has advised the NGIoT consortium on specific topics to be further explored in meetings and webinars, such as the webinars on IoT and digital skills, IoT and open sources, etc. Other topics have emerged from NGIoT's analysis of the available literature and policy papers, as well as from engagements with the wider community.

The webinars and workshops organized so far have ranged broadly from human-centred IoT, to cybersecurity, reference architectures, standards and privacy by design. The discussions and presentations during the workshops and webinars confirm the importance of the research challenges and topics that have been identified in the draft IoT Roadmap for Research, Innovation, and Deployment and are presented in this deliverable. The webinars and workshops also provided important information to further shape the current proposed challenges and trends, as well as move into new directions, as described in NGIoT deliverable 3.2. Future Trends in IoT.

4.5.3 Summary of inputs received from workshops/webinars

This section summarises main input received by NGIoT in relation to future trends for IoT. Inputs have been incorporated in the priorities discussed in Section 5.

4.5.3.1 Evolution of IoT devices

While from a technology perspective, this reduction of energy consumption can be achieved through a combination of hardware and software solutions, some experts advocated a more sober and responsible approach to the digital transformation, where the value for society and humans should be prioritized, rather than the connectivity as such. The human side - as for example, consumer behaviour in relation to connected devices - is an important aspect as well. It has also been suggested that the adoption of low-power emerging non-volatile memory for AI applications, as well as the

implementation of efficient in-memory computing systems, could help minimizing energy consumption in data centers, which are nowadays important consumers of energy.[143]

4.5.3.2 IoT security, privacy and trust

As for many other new technology, understanding how to increase trust toward Internet of Things by end-users should be studied requires a multidisciplinary approach and a gender focus. In this respect, data privacy and safety should be regulated from an ecosystem approach and managed in this complexity with regard to changing roles, various types of data and the reuse of data. Empowering individuals to exercise their rights: Individuals value the high level of protection granted by the GDPR and ePrivacy legislation. However, they suffer from the absence of technical tools, standards and institutions that make the exercise of their rights simple and not overly burdensome.

Expert observed that the EC has already done important work with developing a regulatory framework for AI. A new regulation as a key to clarify the perimeter of application of personal data protection and non-personal data protection legal frameworks, as well as the boundaries of intellectual property would be useful. In the future, the GDPR needs to be updated and adapted to the innovations that will happen in an AI context.

As regards IoT security, experts observed that the new data paradigm where less data will be stored in data centres, and more data will be spread in a pervasive way closer to the user 'at the edge', brings new challenges for cybersecurity. It was also observed that, securing IoT applications is not just about protecting personal data and and business data, it is about protecting people as individuals, as citizens, as users of services Three major area of innovation foreseen include: secure elements; cryptography and Blockchain[144].

4.5.3.3 IoT, data sharing and management

Managing data in a fair and responsible way in ecosystems is necessary but complex, and new institutions for data governance are needed in the future who can handle this complexity. Currently, most of the data is in the hands of corporates, but cities as governance units should work for ownership of their own data and of their citizens.

Experts evidenced the need to think and reinvent the governance of the data economy and invent new institutions for data protection that can handle the issue of ownership with regard to the reuse of data, autonomous IoT solutions an AI. A suggestion is to create data libraries with representative steering boards - a place for people to go to when they have issues with how their data is handled or need an overview.

Data process management is facing challenges related to data quality, data trust, scalability and accuracy, sharing and interoperability, as well as commercialisation.

Experts obsverd that standards play a crucial role in data sharing and should be promoted. They facilitate the digital transformation of cities and communities, but they are also part of the complexity, as hundreds of standards exist in the field of smart cities. However, 'the alternative, the absence of standards, is worse.'

---

[143] DECISION Etudes & Conseil. Study on Emerging Technologies in Electronic Components and Systems (ECS) – Opportunities ahead (2020)

[144] DECISION Etudes & Conseil. Study on Emerging Technologies in Electronic Components and Systems (ECS) – Opportunities ahead (2020)

According to experts, another challenge for cities in their digital transformation is to find a balance between what citizens want and what is scalable. One of the big problems relates to the size of data. Different types of data require different types of processing of data. Managing data in an interoperable way faces contractual complexities, legislation, cybersecurity risks, procurement legislation, privacy legislation, data ethics and societal concerns, and requires digital literacy of end users. Cities have huge amounts of data, but the challenge is the quality data; how to secure real time data, where to store historical data, in which ways urban data can be made available, ownership of data and transparence. An extra effort is needed to achieve data integration standards convergence.

Experts recommended to focus on avoiding vendor lock-in, reducing costs and time to market through interoperable mechanisms to enable foundations for European Data economy. To achieve progress and transform a heterogeneous and siloed legacy infrastructure into interoperable and industrialised smart city services, cities need to work together, with relevant existing networks, such as OASC, EUROCITIES, and with standardisation organisations (ETSI, ITU, CEN-CENELEC).

Open platforms and standards are play a key role to promote establishment of data economy, still the monetisation aspect is often weak he next step of the roadmap for open data platforms is to build the monetarisation part of the platform. So, while open source should be promoted, commercial data is needed to create profit. New business models should be developed to make businesses more coherent and adaptable to open data platforms.

Based on experience, it is unlikely that one single platform will dominate the market. Investment in achieving standards convergence will help moving from vertical silos to data marketplaces that are expected to advance to the centre of the data economy.

This is particularly crucial in some sectors such as Smart Cities: when developing Urban Data Platforms, cities should favour collaboration and interoperable solutions. Considering the larger number of available standards, cities should continue pooling their expertise and work together on interoperability, which is the key for replicability and scalability.

4.5.3.4 IoT and Interoperability

Data interoperability remains a challenge, that, while it may be mitigated by effort in the harmonisation of data models within single domains, will still be present when dealing with legacy systems and cross-domain data exchange. According to the experts, to lay a foundation for a European data economy, interoperability is key, as it avoids vendor lock-in, stimulates the market by giving confidence in the ecosystem as a whole and reduces costs and time to market. Interoperability also helps to ensure citizens' digital rights protection, which is essential in IoT adoption. They also evidenced that to promote interoperability, it is important to leverage on the work of already existing networks, such as Open & Agile Smart Cities (OASC), EUROCITIES, and standardisation organisations , such as ETSI, ITU, CEN-CENELEC. Considering the large number of available standards, key players in the ecosystem should continue pooling their expertise and work together on interoperability, which is the key for replicability and scalability. Scalability should be understood in three ways: in terms of size, in terms of scaling across (cross-border), in terms of scaling deep (learning from data, multi-cloud infrastructures). International agreements on standards should be supported, as they will give more confidence for the public sector and enlarge the market for business. While standards are essential for interoperability, not everything should be standardized. What is important are the pivotal points of interoperability in the southbound and in the northbound. This refers to the starting point of the OASC Minimal Interoperability Mechanisms (MIMs) and links to the Horizon 2020 ESPRESSO project. Mechanims such as OASC's minimal interoperability mechanisms (MIMs) are essential for solving urgent societal challenges at scale. Open source also play a key role in promoting interoperability: ICT reference architectures and interfaces must be defined in a way that open source components can be used. In relation to this, experts observed that new business models should be developed to make businesses more coherent and adaptable to open data platforms and interoperability. They also

evidenced that EU and member states have a role in the governance of interoperability: the governance framework is an urgent matter to address , especially when it comes to deploying new technologies in cities, as many cities still face fragmentation and silo organizational setup.

4.5.3.5 IoT as system of systems

Expert observed that IoT as isolated technology doesn't exist. IoT is always connected with other technologies, producing different outputs, data production, infrastructures etc. The focus should be on how technology is iterated. As data is produced at a high paste and reused in various contexts it is hard for producers and consumers of data to follow and have an overview of how the data will be used afterwards. Reccomendation is to identify the required interaction and integration with technologies. IoT as an assemblage of technologies which has an impact on the users and society in general. There is still huge potential to identify and converge opportunities for a better and more effective use of IoT and other emerging technologies and the focus should especially be on deployment efforts and plans.

This should be reflected also on educational programmes at all levels: programmes should include digital literacy and covers also fundamentals on data protection and privacy already from early grades to ensure empowerment of endusers, but also of future employees.

Digital skills should be promoted in industry, as technology developers are only skilled in certain aspects but do often not have the knowledge to oversee and foresee the usage of technology in future contexts and the impact technology will have on society.

4.5.3.6 IoT role for the European society

According to the experts view, IoT solutions do not use the full potential of the input that end-users can bring in order to make IoT and other technologies more tailored to the demands of society. Citizens and end-users need to be involved in the whole process from idea to commercialisation to achieve the highest societal impact. Empowerment of citizens and instruments that support the participation of citizens is the key factor to a successful uptake of IoT and other digital technologies in cities and communities. For effective involvement of the communities working with citizens' groups that are concerned about a topic can be recommended, especially to define and develop use cases and pilot scenarios of existing and new solutions.

IoT and new technologies should be implemented in cities and communities to serve the goals set in the strategy "The European Green Deal". Extensive uptake and scaling up of digital solutions are crucial to help cities and communities meet their climate targets and reduce their environmental footprint. European initiatives on scaling digital solutions should be promoted. IoT has a major potential to solve societal challenges related to environmental change. The focus should however not be on a single technology, but rather on how various technologies can be combined to solve pressing issues. Climate neutral cities based on a sound digital foundation as a public mission for Horizon Europe Programme should be a core priority. Digital Twins can make major contributions towards achieving Global Sustainable Development Goals and The Paris Climate Agreement. This includes improvement of decision making using predictive data, increasing awareness, Timely and efficient feedback on the impact various environmental phenomena can cause, monitoring change and building foresight scenarios.

As ICT itself count for 8-10% of electricity demand, uses rare earths resources and produces waste, the vision should be to strive for a sober and responsible digital transformation of society and initiatives taken (Edge & open source) to address the accelerating resource demand due to a fast increase in connected devices.

In this respect, partnerships between cities, implementing IoT and other new technologies to fight climate change is key, as well as partnerships across sectors and organisations. For example, testbeds

and Living Labs for IoT and other technologies with a green focus should be established across European cities and regions.

5 IOT RESEARCH, INNOVATION AND DEPLOYMENT PRIORITIES

5.1 Challenges & Topics

As result of the analyses of different roadmaps and the engagement with the community at different events, and taking into consideration the latest disruptive technologies, NGIoT identified the following high-level research challenges for the next work programmes. Priorities identified cover different aspects of the IoT stack and, accordingly, relate to other transversal research and technologies, including: 5G, Distributed Ledgers, Big Data, Artificial Intelligence, Cyber Security, and Cloud Computing. Some of the priority challenges go beyond pure technological research and require a holistic approach to take into consideration research in sociology, anthropology, economy, neurology, biology and ethics.

5.1.1 Foundational challenges

5.1.1.1 Reliable, low-cost, sustainable and scalable IoT networks (R1).

While LPWAN solutions have been largely tested and offer a low-cost solution for large IoT deployments, they suffer several drawbacks in terms of supporting real-time and high-bandwidth scenarios. Despite the fact that NB-IoT and LTE-M appear to be initial solutions to the open challenge, they fail in some respects. On the one hand, NB-IoT, designed with increased reach and lower cost and power consumption, offers limited bandwidth and latency around 1 sec. On the other hand, LTE-M, while providing higher bandwidth, fails on the low-cost constraint. This implies that the road to provide large-scale deployment, able to support real-time scenarios with bidirectional communication at a low cost, is still a challenge. 5G and its evolution should go further to address the low cost, massive device deployment. Such technologies need as well to be sustainable by limiting the usage of resources and the impact on the environment, to avoid the large-scale deployment of devices becoming unsustainable from an environmental point of view. The forecasted increasing number of devices we will witness in the future will make this challenge more pressing. This challenge relates to optimizing IoT integration into the global Internet, with a focus on IPv6, as well as in cellular networks, such as 5G (and other future networks), but it entails as well research in relation to energy and sustainability of IoT devices.

As part of this challenge, NGIoT identified two major topics:

- **R1.1 - Low-cost, high-volume connectivity.** This research topic focus on exploring radio transmission solutions that, while increasing bandwidth available for IoT data transport, would reduce the cost of deployment of the radio networks. Research should evaluate new frequency bands (e.g. unlicensed band > 200 GHz), new medium for signal propagation (e.g. single mode optical waveguide using laminated polymer platform). Light Fedelity communication technology and its convergency with 5G should be further explored as well.
- **R1.2 - Low-power connectivity schemes.** This research topic focus on hardware and software solutions that drastically reduce the energy consumed by IoT devices to collect and transmit information. Software solutions and communication protocols may optmise activation of communication and consumption during communication, while energy harvestor and other bio-inspired solution may increase the capacity of batteries and energy independence of devices.

The key enabling technologies for this challenge are:

- **5G/6G**

- **Advanced electronics**

5.1.1.2 Next Generation IoT data processing architectures (R2).

The Internet of Things (IoT) is one of the key drivers of the Big Data phenomenon. IoT was one of the main drivers for the switch from batch analytics to real time analytics solutions. Still, while a plethora of real-time processing solutions and platforms are available today on the market, it is clear that the amount of data generated is growing faster than the processing capacity, and often poses a real challenge to the storage capacity. This hinders the ability to generate value from sensors data in real-time and also as batch processing, given that it is not always possible to retain and store all the generated data. Current research and development trends to solve this challenge focus on the so-called edge computing architecture. This architecture solution, while it is able to cope with today's needs, applying the 'divide et impera' principle leveraging existing data processing solutions, may not be enough for future needs. Most probably, real-time analytics architectures will need to be retaught, and their functions - to increase their speed - will need to be directly available at the level of processing units (this trend is already being explored by some activities in the FPGA research). In short, IoT data processing architectures need to be scalable by design.

As part of this challenge, NGIoT identified three major topics:

- **R2.1 Novel data processing architectures.** With the advent of edge computing, data processing is becoming more distributed and decentralised. Most of the data processing solutions in place today are cloud-native and assuming a centralised processing. While first steps are ongoing to deliver such architectures, these are evolutionary solutions, i.e. extension of existing technologies and approaches to incorporate edge processing. This research area should explore novel mechanism for data processing, looking beyond current consolidated solutions. In this sense, an interesting paradigm to start from is surely function as a service in its recent evolution including edge-cloud orchestration and in memory-databases.
- **R2.2 IoT data processing optimised micro processing units**. This research topic deals with the development of processing units specialised on IoT data processing task, including native support for machine learning and deep learning functions (cf. R6.2), thus increasing the throughput at the edge of the processing of IoT data for localised data intelligence. Current research shows than AI specialised processors can achieve 10 time the performance of GPUs and FPGAs. While achieving this goal, research should also ensure that energy usage is keep under control (cf. R1.2)
- **R2.3 Highly scalable and low latency ledgers for IoT.** In more and more IoT scenario, distributed ledgers are key enablers for secured and trusted data exchange and distributed processing. However, their application in real time scearios is still not possible given that current distributed ledger solutions introduce additional latency in the data management and have high computing costs. Proper solutions need to be explored to allow adoption of distributed ledgers at the scale and latency required by real time IoT scenarios.

The key enabling technologies for this challenge are:

- **Artificial Intelligence and analytics**
- **Distributed Ledgers**
- **Edge computing**
- **Advanced electronics**

5.1.1.3 Futureproof security and trust (R3).

While there is a plethora of past and ongoing research on security in the IoT field, the constant and rapid evolution of IoT technologies and cyber-attacks, requires consistent investment in these areas. In this respect, research should focus on 'intelligent' approaches to the security, i.e. on the ability to 'learn' new attack patterns and derive counter solutions autonomously. Beyond cyber security for IoT, trust toward IoT solutions and data generated by devices is becoming an important trend in the market. Solutions are focused on providing ways to produce and consume IoT data by highly decentralised and loosely coupled parties through secure traceability mechanisms such as blockchain. Still, current blockchain solutions are far from tackling scalability requirements posed by real-time data scenarios in several IoT market segments. It is important to highlight how trust is an essential aspect for the human interaction with IoT-enabled services, and goes beyond pure technological aspects, encompassing also psychology, sociology and ethics research.

As part of this challenge, NGIoT identified two major topics:

- **R3.1 Novel future proof cybersecurity.** Research in cyber security explored supervised and unsupervised machine learning methods such as Random Forest (RF), SVM (Support vector machine), decision trees (DT), k-nearest neighbour (KNN), k-means, Principal component analysis (PCA) and association rule (AR) algorithms have been widely adopted in cyber security. Their ability anyhow to detect an attact is strictly related on the attack patterns identified in the past. More recently, initial attempts to leverage deep learning and reinforce deep learning provided interesting results in the identification of IP Spoofing and DDOS. Such methods seem promising since they have been able to recognize attacks that were not showing similarities with previous attack patterns. Research in these direction is key to increase resiliency of IoT platforms.
- **R3.2 IoT data traceability and trust.** Data traceability is key step to increase trust over data. In particular, taking into account security concerns linked with IoT devices, the tracing provenance of data and the usage of solutions that guaranteed that darta have not been tampered is essential to increase trust toward IoT systems. Distributed ledgers are becoming the reference solution for data traceability in different scenarios, including, for example food provenance and circular economy. While distributed ledgers have been applied to IoT to increase trust, current protocols are still limited in term of scalability when it comes to large scale sensor networks. Higher scalability of consensus protocols are needed for IoT. Different solutions are promising, including the ones explore by EU initiatives such as IOTA, and mixed approaches that combine ledgers with DHT overlays (e.g., Chord, Pastry, and Tapestry).

The key enabling technologies for this challenge are:

- **Artificial Intelligence and analytics**
- **Distributed Ledgers**
- **Cyber Security**

5.1.1.4 IoT, processes, and data Interoperability (R4).

While eventually, as in other technology fields, some standards (de facto or actual) will finally prevail regarding integration among devices and platforms, data interoperability will remain a challenge, that, while it may be mitigated by effort in the harmonisation of data models within single domains, will still be present when dealing with legacy systems and cross-domain data exchange. This would result in increasing costs on the integration of IoT solutions. While several technologies promised automated semantic interoperability in the past, this is still far from being achieved. Still, a pragmatic approach,

where semi-automatic interoperability is achieved through limited human interaction, seems possible with today's technologies. While data interoperability is a requirement to enable cross-domain applications, an even more complex aspect that requires attention is the ability to orchestrate business processes across domains. Processes enacted within IoT and data platforms may be much more complex to interoperate than data, thus, enabling the interoperability between cross-domain platforms requires solutions beyond data interoperability. Past research in the field, e.g. semantic business processes, showed little scalability and applicability - novel scalable and reliable solutions are required.

As part of this challenge, NGIoT identified three major topics:

- **R4.1 IoT data dictionaries deployed at scale**. One of the key solutions to ensure intereoperabilty of IoT solutions, is the adoption of common and standardised dictionaries. While a number of efforts taclked the definiont of such dictionaries in relevant scenarios, the coverage of scenarios is still limited, and worst the adoption of such dictionaries is often limited. Activities should focus on increasing available dictionaries and their adoption.
- **R4.2 Semi-automated data interoperability.** Several IoT solutions deployed on the market are specific to a given domain. This trend contributed to creation of so called data silos. This makes quite complext the seamless integration and intelligent analysis of the various heterogeneous data sources. In the past solutions based on semantic technologies have been proposed, and while they worked well conceptually, the had several issues of scalability and performance. With current evolution of deep learning techniques should be explored to provide automate as much as possible annotations and transformations.
- **R4.3 Semi-automated process interoperability.** If attempts to automate data interoperability proved so far uneffiient and not scalable, the state of the play for processes it is even more complex. Still, such interoperability is key to increase the dynamic integration of different IoT platforms enabling ecosystem of IoT data consumption and production.

The key enabling technologies for this challenge are:

- **Artificial Intelligence and analytics**

5.1.1.5 IoT, Citizens, Privacy-by-design, and Ethics (R5).

While most of the challenges discussed above have a primary focus on technology, there is an important challenge unrelated to technology that needs proper attention for the development and adoption of Next Generation Internet of Things solutions. It is clear that the wider the adoption of IoT, the wider the 'intrusion' of devices and 'intelligent' services will be in our everyday life. What is an acceptable level from a citizen's perspective? What are the ethical implications that Next Generation Internet of Things solutions need to face? How it is possible to make what happens behind the curtains more transparent to ensure that intelligent solutions can be trusted? How can such solutions ensure compliance with GDPR, as well as with future regulations in this field? How can citizens be truly aware of the decisions they are making within respect data processing? How can we ensure an inclusive approach to IoT and counteract possible inequalities that might emerge with the wide adoption of IoT? And as connectivity intensifies, citizens will increasingly request spaces of disconnection. How can we facilitate these requests? This challenge is clearly demanding for a multidisciplinary approach embracing legal, sociological and ethical research in relation to the adoption of IoT and connected technologies, such as Artificial Intelligence.

As part of this challenge, NGIoT identified two major topics:

- **R5.1 Privacy-by-design for IoT devices.** Devices are considered one of the more exploitable entry doors for cyber attacks. Thus it is essential to advance research related to their security, including solutions for on-chip encryption, hardware-software integrated security functions, tamper proof technologies.
- **R5.2 Security & Privacy-by-design for IoT services.** Recently there have been more and more breaches of sensitive data, and attacks on critical infrastructures. Increase security of IoT infrastructures is central to the safety and security of several applications and their users. On the security side, it is fundamental that research strengths methods for development of secure architectures including new methods and tools for formal verification of specifications, designs and implementations to detect possible security threats. Artificial Intelligence may play a key role into supporting such methologies and in the development of cyber threat solutions (cf. R3.1). (model level proofs, source code analysis, binary analysis, hardware analysis, etc). As regards privacy, many research aspects are yet to be explored, including: ways to automate GDPR compliance tests, solutions to provide privacy preserving data processing and machine learning (for which distributed ledgers may provide interesting solutions), mechanism to generate dynamically data access control policy based on different context parameters while preserving data privacy.

The key enabling technologies for this challenge are:

- **Artificial Intelligence and analytics**
- **Cyber Security**

5.1.2 Emerging challenges

5.1.2.1 Real time decision-making for IoT (R6).

While a plethora of solutions are available for deriving knowledge from data, IoT poses a new level of challenges to machine learning and its recent evolutions (the so-called deep learning wave). Coordinating real-time decision-making based on a widely distributed and decentralised infrastructure, so as to achieve a common goal, is not trivial. Despite being not trivial, this ability is a key enabler for different scenarios that are becoming more and more relevant for the market, like in the use case of self-driving cars. In several of these scenarios, decision-making will also need to take into account the 'human' factor, and the underlying ethical aspects, including the obstacles that lack of trust may pose to such solutions (which is a general concern in AI-related research). This challenge relates encompasses ethics, socio-economic and psychology research.

As part of this challenge, NGIoT identified four major topics:

- **R6.1 Dynamic orchestration of decentralised AI pipelines.** With the advent of edge computing, AI processing is moving from the cloud toward the edge, allowing for fast local decisions. To make this possible it is key to explore intelligent mechanisms to orchestrate AI pipelines, i.e. the process of collecting and adapting data for model computation, the model computation and their deployment. Such pipelines will need to have ways to define conditions to trigger model re-computation and ways to preserve data privacy in complex and distrinbuted IoT ecosystems (e.g. by leveraging federated machine learning architectures)
- **R6.2 Native AI-capable devices.** As discussed in R2.2, to improve performance of IoT-related data processing and decision making, developing devices with novel processing capacities is key. In particular, advancements in AI specialised processors are required. In this field,

Neuromorphic computing seems promising thanks to its principle of mimicing neurons to learn and compute.

- **R6.3 AI for Humans: understandable and ethical decisions.** While humans could easily understand first AI systems, recently the adoption of deep learning models such as Deep Neural Networks (DNNs) is raising and increasing the opacity of AI systems. At the same time, users interfacing with AI systems are more and more demanding for transparency. To answer this need, research focused on eXplainable AI (XAI). XAI leverages social sciences (e.g. psychology) to define a suite of machine learning solutions that produce easy to explain models so as to enable their understanding by humans. Making models human understandable is the first step toward trust of AI and ensuring its compliancy with ethics, i.e. toward responsible AI. Research in XAI and similar approaches required advancemnts in order to achieve same performance as "black-box" machine learning systems and increase the adoption in IoT solutions.
- **R6.4 Validated AI algorithms for IoT use cases.** While there are a number of models discussed in research papers in relation to different use cases (e.g. pest detection in agriculture, object and vehicles identification in smart mobility) rarely these template models are tested at scale and made available freely and openly. Stakeholders capable of generating (or having access to) large enough data sets to compute accurate and efficient AI models are generally keeping them closed source, thus limiting the impact and benefit for society and the possibility to verify and validate the models (also within respect ethics issues). To the aim of releasing to the wide public free and open high quality AI models, a singergy with data market places is key (cf. R9.2).

The key enabling technologies for this challenge are:

- **Artificial Intelligence and analytics**
- **Edge Computing**

5.1.2.2 Autonomous IoT solutions (R7).

Maintaining an IoT infrastructure, spanning from the platform to the sensor layer, is a complex task. While nowadays there are a plethora of solutions helping resource orchestration (relying on the development of principles largely adopted by cloud platforms), the room to increase automation is still large at each level of the stack. Beyond that, autonomous IoT systems may be able to transform C-level KPIs into corresponding actions at the different layers of the IoT stack, thus reducing time to implement C-level decisions. In this sense, the most promising trend is the adoption of novel Artificial Intelligence techniques in combination with latest virtualisation trends proposed by 5G research to ensure a higher-level degree of self-automation by IoT technologies, from the sensors through the transport network, the gateways and up to the platforms. Another correlated challenge comes from the maintenance cost of IoT deployments, which is directly linked to the energy efficiency and autonomy of IoT solutions.

As part of this challenge, NGIoT identified two major topics:

- **R7.1 Large IoT & digital infrastructures.** Within Europe there is yet a lack of large deployments of IoT networks and digital infrastructures in general. This, beside slowing down the digitalisation process, also limits the ability to understand and test pratically implications of very large real life deployments of IoT infrastructures. This also relates to the unavailability of widely distributed public edge infrastructures that would allow to benefit OPEX model to IoT edge infrastructure investments. A potential research direction would be enablement of edge-federations and edge resource sharing solutions.

- **R7.2 Semi-autonomous IoT infrastructures / R7.3 Autonomous IoT infrastructures.** Due to the heterogeneous nature of the IoT infrastructure, which includes a variety of edge nodes with different resources, capabilities, mobility, ownership, etc. managing and operating IoT infrastructure at scale is more and more complex. Research is required to increase the automation in the whole cloud-edge-device management continuum to increase efficiency and reliability of IoT infrastructures. Machine learning and Artificial Intelligence may provide essential instruments to achieve such automation. It is important to evidence that IoT is introducing novel requirements to the cloud-edge continuum management, given that in more and more scenarios, IoT solutions may become dynamic ecosystems, thus required dynamic composition of edge resources from multiple owners. Such composition should occur preserving isolation of different users and privacy of data by the different stakeholders leveraging shared edges.

The key enabling technologies for this challenge are:

- **Artificial Intelligence and analytics**
- **Edge Computing**
- **5G**

5.1.2.3 Human and sustainable development in the loop IoT (R8).

While several IoT and CPSs solutions are intended to serve humans, most of the IoT solutions we witness today are still designed for M2M communication. Thus, the support for interaction with humans, and the enablement for them to take decisions and interact with the systems is often limited. While we have witnessed the usage of humans as “sensors”, most of the existing solutions still consider the human as an external and unpredictable element to the IoT system control loop. Research in the direction of including the human element in IoT technologies is key and should take into consideration human intents, psychological states, emotions and actions inferred through sensory data. In this respect, also the research on the Digital Twin concept will have a key impact, enabling humans to perceive IoT systems more related to their physical counterpart. This challenge is clearly demanding for a multidisciplinary approach combining Artificial Intelligence, ethics and psychology research. Similarly, IoT can play an important role in achieving sustainable development, including the UN Sustainable Development Goals (SDGs).

As part of this challenge, NGIoT identified three major research topics:

- **R8.1 Sustainable IoT by design**. A sustainable approach to IoT requires exploring solutions such as low power IoT devices and novel technologies for environmentally sustainable devices and sensors. Recent research also took into consideration the service side of resource efficiency, bringing into the picture energy-aware IoT service composition. “Sustainability” of course has a broader meaning and, in the case of IoT, covers as well other important aspects as well, such as resilient infrastructures, and inclusive access to technologies. So far research gave little attention to holistic approaches aiming at understanding how the different components of an IoT ecosystem contributes to make it sustainable, scoping from technologies to policies. Research should focu on study how the different layers of an IoT ecosystem can interplay to deliver sustainable IoT solutions, it should explore how systems can self-adapt to comply with sustainability KPIs. Innovative ways to incentivize Sustainable IoT policies are also to be explored.
- **R8.2 Augmented IoT.** While augmented reality technologies are maturing, their adoption in conjuction with IoT is still limited. The relevance of Augmented Reality for IoT is linked to the ability to allow humans to interact with data generated by IoT devices and devices themselves

in a similar way to the one humans would interact with the physical world by "augmenting" it. The combination of Augmented Reality with Internet of Things and Artificial Intelligence to support human control and interact with "things" is still at its infancy and its key to for the development of advanced Digital Twin solutions. Research should explore not only solutions to enable Augemented IoT, but also socio-ethical aspects linked with the transition toward such novel type of interactions with the physical world.

- **R8.3 Tactile Internet.** Human sense are able to interact with the physical environment at incredible speeds. While a muscular reaction is in the range of 1sec, human visual reaction is in the range of 10 msec. Thus while interacting with "things" humans expact reaction times compatible with their senses capacities. Tactile Internet research explore solutions to provide such "low latency" and "human-sensible" interactions (e.g. leveraging haptic feedback) with the ultimate goal of empowering humans to control remote "things" via Internet like real physical objects. Tactile Internet thus enables precise human-to-machine and machine-to-machine interaction key to several scenarios such as in manufacturing or in healthcare. Requirements of the Tactile Internet place extraordinary demands on networks' latency and reliability, security, IoT architecture, sensors and actuators. Research in the area is still in its infancy and 5G/6G research progress are not yet at point of providing end-to-end latency below 1 msec in remote control loops, still relevant progress in research for haptic interactions and augmented interactions have been done. Leveraging on Photonics technology to reduce latency in both the communication and sensing/interaction layer may be key to achieve the Tactile Internet vision.
- **R8.4 IoT for sustainability.** IoT-based solutions can improve the sustainability of different economic sectors such as manufacturing, agriculture, and smart cities. This line has been deeply explored and the applicability of IoT to improve efficiency of processes and reducing resource usage, is now considered a fact. Research exploring impacts on other scenarios, such as social inclusion, is starting to take up as well with major focus on impaired and ageing people.

The key enabling technologies for this challenge are:

- **Artificial Intelligence and analytics**
- **5G**
- **Edge computing**
- **Augmented Reality and Tactile Internet**
- **Digital Twins**

5.1.2.4 IoT data sharing and monetisation enabling models and technologies (R9).

While different IoT Data Markets are starting to go live recently, their appeal in the market still seems limited. This is mostly due to two factors: i) the scale of the available data in these data markets that is often limited and hence only of interest for a limited set of stakeholders; ii) the actual value of the data on the market, that being mostly raw data, has limited value for potential buyers. The first issue is mainly driven by the fact data owners are not motivated to share data for different reasons: e.g., a loss of data control, lack of adequate incentives, and a lack of trust toward intermediary platforms. The second issue is related to the fact that most of the platforms, not having enough data in place, cannot offer actual added value on top of the raw data provided by data owners. Latest trends in the data-sharing technologies show how Distributed Ledgers can increase trust toward data sharing and increase the feeling of data control by owners. This challenge, despite its relation to different

technology fields, is mostly a socio-economic challenge related to the development of proper business models fostering the creation of larger IoT data markets.

As part of this challenge, NGIoT identified three major research topics:

- **R9.1 IoT data market architectures.** Differently from centralised data market architectures that can be applied in several scenarios, in the case of IoT scalability may be achievable only with decentralised and distributed approaches. Distributed ledgers, while offering a decentralised approach and providing solutions increasing data control by owners, have yet to mature and achieve performances required by realtime IoT scenarios. Efforts and experiments have beed done in this direction, for example, by IOTA and Streamr to develop IoT data market places based on IoT native distributed ledgers.
- **R9.2 Novel business models to incentivise data sharing.** While data sharing could provide huge benefits to the whole society, successful examples of data market are very limited. Sensor data sharing markets such as Streamr, Dawex, and QueXopa are still low populated. Companies are reluctant to sell their data, since they cannot easily evaluate the monetary value of the data to the purchaser and consequently are afraid of setting a price. Another, perhaps more obvious reason is that many companies are afraid of their data being used against them. In the data economy context, platform cooperatives have been proposed and implemented with the purpose of tilting the asymmetric distribution of power to affect platform rules, and the distribution of value, towards more symmetric and equitable arrangements. Often the value of the data cannot be determined when a data provider and data consumer agree on the use of the data, but only when the data are actually used by the data consumer. These demands for new governance models - or new kinds of agreements - that define how the value of the data is evaluated at the time of its use, how the created value is shared or divided, and what are the rules for the parties for extracting or monetizing the value. This may lead to new compensation models different from the typical one-the-spot monetary compensation.
- **R9.3 Large data marketplaces for IoT scenarios.** While as mentioned above IoT data marketplaces have been experimented in different use cases, so far they haven't reached the critical mass that would allow them to generate value for the stakeholders involved. Public investements, such as the ones envisioned in the EU Data Strategy, may be able to mobilize the scale needed to create such market and make them sustainable.

The key enabling technologies for this challenge are:

- **Distributed Ledgers**
- **Edge computing**

5.1.2.5 Sustainable and biocompatible devices (R10)

Recent advancements in biotechnologies and nanotechnologies should be exploited to experiment the development of IoT devices that dramatically reduce energy consumption (increasing their lifespan) and the development of sensors that are biocompatible (and hence to do not pollute environment) and aim at biodegradability.

As part of this challenge, NGIoT identified three major research topics:

- **R10.1 Energy (semi)-autonomous devices.** Early studies indicate that the combination of micro-energy harvesting and micro-storage technologies may be the future for long lasting IoT devices. Improving their combined performance while downscaling their size can only be achieved through breakthroughs in materials performance and system architectures that allow for high density features and embedded energy options in integrated circuits (ICs) .

- **R10.2 Bio-compatible sensors.** Recent research showed the great potential for the improvement of the devices design holding by nano- and biomaterials invented in the last decade. Research should advanced toward minimally invasive electronic devices embedded directly into biological objects. Such hybrid systems may enable high-quality, low-cost sensors as an alternative to more expensive fully electronic devices. IoT applications will benefit from using hybrid bio-electronic sensors which rely on natural capabilities of bio objects (e.g., bacteria, plants, animals) and react to changing environments.

The key enabling technologies for this challenge are:

- **Advanced electronics.**

5.2 Priority Verticals and Application Domains

While it is outside the objective of the scoping paper to define application domain specific challenges in relation to IoT (the list would be too long), some of the challenges listed above are fundamental for some application domains. Links between domains as discussed in Section 3, and Research priorities are listed in the table below.

Domain	Top Related Research Priorities	Description
Agriculture and Smart Farming	• Reliable, low-cost, sustainable and scalable sensor networks (R1) • Real time decision making for IoT (R6) • IoT Data Sharing and Monetisation enabling models and technologies (R9)	IoT adoption in Smart Farming is still limited. This is mostly related to the costs of the infrastructure and to benefit not being clear. In this sense, predictors based on IoT data can play a fundamental role. Such predictors demand for large amounts of data to be available to compute them, thus the incentives to make such data available are needed.
Healthcare	• Future-proof trust and security (R3) • Human-in-the-loop IoT (R8) • IoT, citizens, privacy & ethics (R5)	On the one side, health data are sensitive data, which poses several ethics, privacy, trust and security questions for IoT solutions. On the other hand, a better evolution of IoT technologies in the medical field, especially within respect to their interaction with human factors, can revolutionize the healthcare sector.
Energy Management	• Real-time decision making for IoT (R6) • IoT Data Sharing and Monetisation enabling models and technologies (R9)	The ability to optimise in real time energy resources is key in the sector. To create fine optimised models for the purpose, it is fundamental to be able to share and access data across the different stakeholders in the energy market.

Domain	Top Related Research Priorities	Description
Manufacturing	• Reliable, low-cost, sustainable and scalable sensor networks (R1) • Next Generation IoT data processing architectures (R2) • Real time decision making for IoT (R6) • Autonomous IoT solutions (R7) • Future proof trust and security (R3) • Human-in-the-loop IoT (R8) • IoT & Data Semi-automated Interoperability (R4)	Manufacturing is a key industry sector where IoT can play a major role. Still, the cost for large deployment of sensors (as needed by complex production plants) and the complexity of managing such sensors and data coming from them, constitute an entry barrier, Also, in this sector security and trust have a primary importance. Beyond that, smart manufacturing requires the integration of a plethora of different data sources and providers, thus increasing automation in the interoperability (of data and processes) will be key to increase IoT adoption.
Media	• Reliable, low-cost, sustainable and scalable sensor networks (R1) • Human-in-the-loop IoT (R8) • IoT, citizens, privacy & ethics (R5)	The wide adoption of sensors in the media sector requires a reduction of the costs of deployment. Beyond that, the media sector is human/consumer centric. As such, it poses a number of ethical, privacy, trust and security questions on IoT solutions. On the other hand, a better evolution of IoT technologies in the media field, especially with respect to their interaction with human factors, can revolutionize the media sector.
Insurance	• Real time decision making for IoT (R6) • Human-in-the-loop IoT (R8) • IoT, citizens, privacy & ethics (R5)	IoT adoption in the insurance industry may lead to new models of risk assessment (including a user's credit & claims history, and the size and type of property owned etc.). This poses a number of ethical, privacy, trust and security questions on IoT solutions.
Transportation	• Reliable, low-cost, sustainable and scalable sensor networks (R1) • Next Generation IoT data processing architectures (R2) • Real time decision making for IoT (R6)	Mobility is a sector that can benefit enormously from IoT. Related deployment costs are still too high for real-time decision-making.

Domain	Top Related Research Priorities	Description
Safety & Defence	• Reliable, low-cost, sustainable and scalable sensor networks (R1) • Next Generation IoT data processing architectures (R2) • Real time decision making for IoT (R6)	Several emerging Safety & Defence scenarios are demanding for more innovative solutions. IoT capabilities can deliver greater survivability to the police officers or first responders, while reducing costs and increasing operation efficiency and effectiveness. The key aspects in these scenarios are affordability and reliability, while at the same time ensuring faster decisions that can save human lives.
Smart cities & communities	• Reliable, low-cost, sustainable and scalable sensor networks (R1) • Real time decision making for IoT (R6) • IoT & Data Semi-automated Interoperability (R4) • Human-in-the-loop IoT (R8) • IoT Data Sharing and Monetisation enabling models and technologies (R9) • IoT, citizens, privacy & ethics (R5)	Smart Cities are increasingly working toward co-creation with citizens and businesses, by combining public and private sensors data. On the one hand, this requires tackling privacy and ethical issues, on the other, this requires that IoT systems take more consideration of human-based interactions. Cities, as shown by initiatives such as OASC, give primary importance to harmonised data models, but it remains unclear how it is possible to incentivize data sharing, bringing businesses and citizens into the loop. Moreover, large deployment for certain scenarios (e.g. public transport tracking) still have prohibitive costs.

Among the above domains, the priorities, according to the NGIoT Research and Development Survey, are: Transportation, Smart grid and energy efficiency, and Smart cities & communities.

5.3 Timelines: from research to mature solutions

In the previous section we identified research, innovation and deployment priorities according to our analysis. To analyse the maturity of research in the above topics and hence define their evolution in the next future we leveraged on the insights from IoT Analytics[145], Gartner[146], ARTEMIS-IA[147] and stakeholders feedbacks.

[145] IoT Analytics. 40 emerging IoT technologies you should have in your radar (2019)

[146] Gartner. Hype Cycle for the Internet of Things (2019)

[147] AENEAS, ARTEMIS-IA and EPoSS. ECS Strategic Research Agenda 2020 (2020)

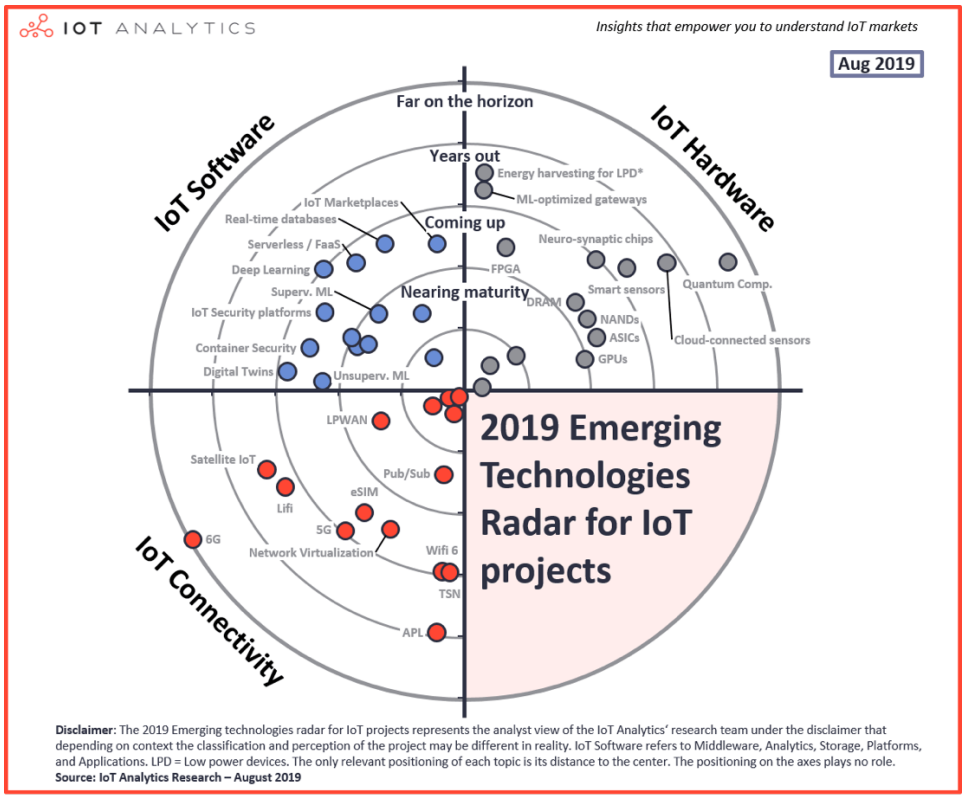


Figure 12. 2019 IoT Emerging Technology Radar[148]

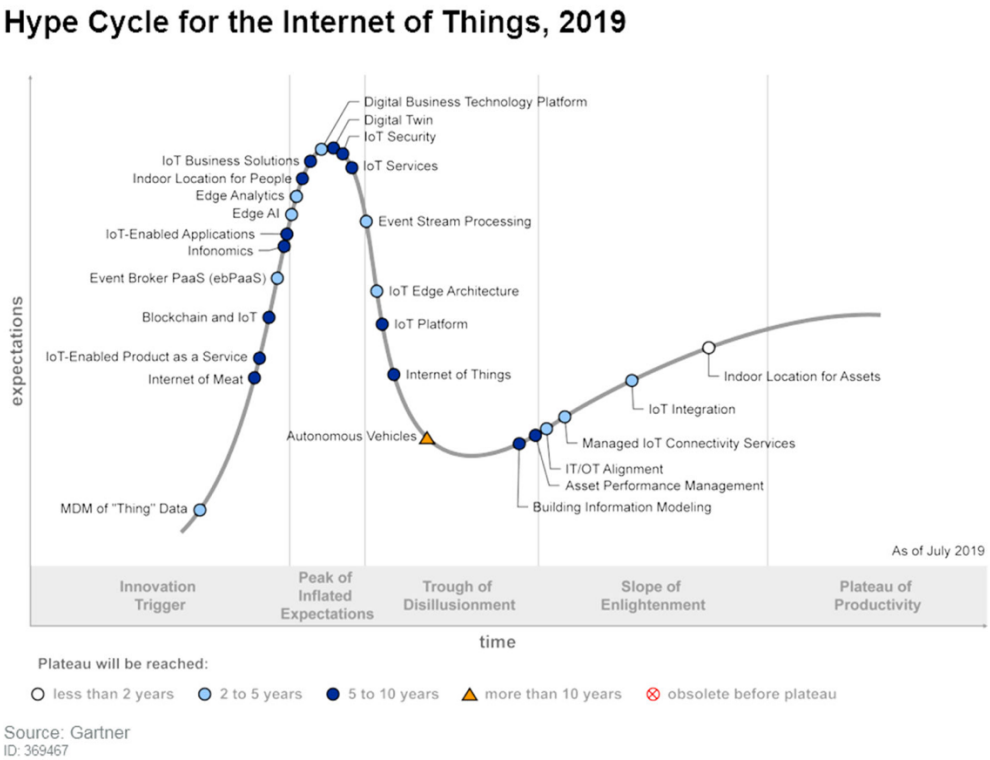


Figure 13. Hype Cycle for the Internet of Things, 2019[149]

[148] IoT Analytics. 40 emerging IoT technologies you should have in your radar (2019)

[149] Gartner. Hype Cycle for the Internet of Things (2019)

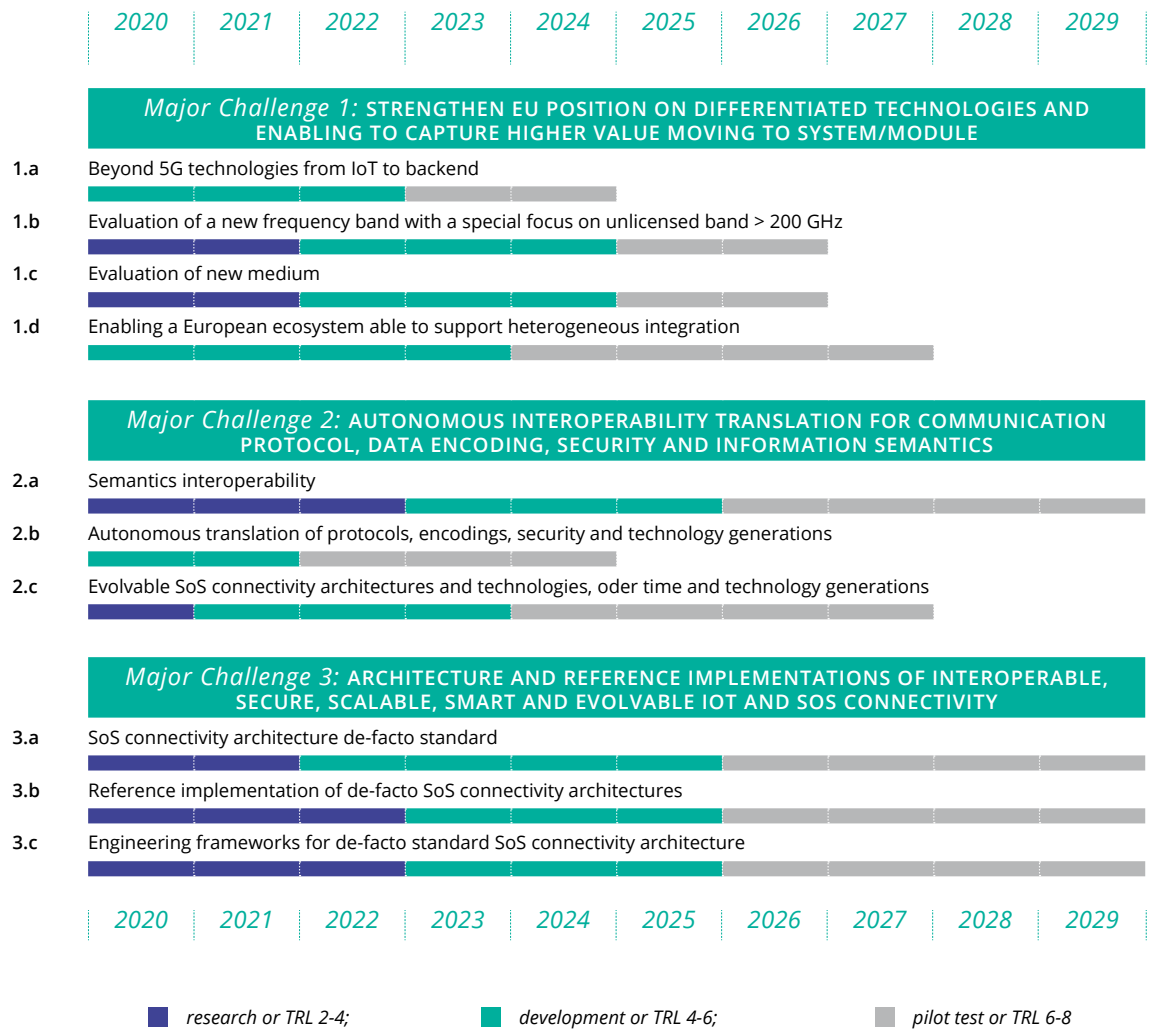


Figure 14. ECS Challenges time frame for Connectivity and Interoperability[150]

Table 2 presents the timeline of R&I&D priorities over the period 2021-2027 highlighting the expected maturity: research or TRL 2-4 (), technology development and field test or TRL 4-6 () and pilot tests or TRL 6-8 (). The table also reports the key technology enablers for each of the priorities. Timeframe has been selected taking into consideration the scope of the upcoming work programmes part of the new MFF. Obviously, taking into consideration the rapid evolution of digital technologies, the medium-term (2023-2024) and longer term (2025-2027) timelines will require additional updates and reassessments in the future.

[150] AENEAS, ARTEMIS-IA and EPoSS. ECS Strategic Research Agenda 2020 (2020)

Table 2. R&I&D priorities timeline for IoT over the period 2021-2027.

: research or TRL 2-4, : technology development and field test or TRL 4-6, : pilot tests or TRL 6-8.

Priority	Timeline							Key enablers
	2021	2022	2023	2024	2025	2026	2027	
R1. Reliable, low-cost, sustainable and scalable IoT networks								
R1.1 - Low-cost, high-volume connectivity								• 5G/6G • Advanced electronics
R1.2 - Low-power connectivity schemes								
R2. Next Generation IoT data processing architectures								
R2.1 Novel data processing architectures								• Artificial Intelligence and analytics • Distributed Ledgers • Edge computing • Advanced electronics
R2.2 IoT data processing optimised micro processing units								
R2.3 Highly scalable and low latency ledgers for IoT								
R3. Futureproof security and trust								
R3.1 Novel future proof cybersecurity								• Artificial Intelligence and analytics • Distributed Ledgers • Cyber Security
R3.2 IoT data traceability and trust								
R4. IoT, processes, and data Interoperability								
R4.1 IoT data dictionaries deployed at scale								• Artificial Intelligence and analytics
R4.2 Semi-automated data interoperability								
R4.3 Semi-automated process interoperability								
R5. IoT, citizens, privacy-by-design, and ethics								

Priority	Timeline							Key enablers
	2021	2022	2023	2024	2025	2026	2027	
R5.1 Privacy-by-design for IoT devices								• Artificial Intelligence and analytics • Cyber Security
R5.2 Security & Privacy-by-design for IoT services								
R6. Real time decision-making for IoT								
R6.1 Dynamic orchestration of decentralised AI pipelines								• Artificial Intelligence and analytics • Edge Computing
R6.2 Native AI-capable devices								
R6.3 AI for Humans: understandable and ethical decisions								
R6.4 Validated AI algorithms for IoT use cases								
R7. Autonomous IoT solutions								
R7.1 Large IoT & digital infrastructures								• Artificial Intelligence and analytics • Edge Computing • 5G
R7.2 Semi-autonomous IoT infrastructures								
R7.3 Autonomous IoT infrastructures								
R8. Human and sustainable development in the loop IoT								
R8.1 Sustainable IoT by design								• Artificial Intelligence and analytics • 5G • Edge Computing • Augmented Reality and Tactile Internet • Digital Twins
R8.2 Augmented IoT								
R8.3 Tactile Internet								
R8.4 IoT for sustainability								

Priority	Timeline							Key enablers
	2021	2022	2023	2024	2025	2026	2027	
R9. IoT data sharing and monetisation enabling models and technologies								
R9.1 IoT data market architectures								• Distributed Ledgers
R9.2 Novel business models to incentivise data sharing								
R9.3 Large data marketplaces for IoT scenarios								
R10. Sustainable and biocompatible devices								
R10.1 Energy (semi)-autonomous devices								• Advanced electronics
R10.2 Bio-compatible sensors								

5.4 From technology evolution timeline to inputs for the future work programmes

To translate the above timeline into priorities for the upcoming work programmes, we have:

i) Grouped such topics within the challenges and mapped them on a timeline corresponding to upcoming work programmes' timelines, i.e. 2021-2022, 2023-2024 and 2025-2027;

ii) Mapped them to research, innovation and deployment based on the current or forecasted maturity;

iii) Associated them with key research topic that are part of the H2020 work programme: Internet of Things (IoT), Cyber Physical Systems (CPS), Cloud Computing (CC), Machine Learning (AI), Data Management (DM), Distributed Ledgers (DL), Networks (5G), Cybersecurity (CS) and Human Computing Interaction (HCI).

As regards the adoption of novel research outcomes in IoT, we have considered the time needed to reach a minimal maturity that would allow them to be adopted in other areas, thus such technologies are associated with IoT only following early development stages.

This should offer the European Commission an actionable tool to support the definition of key topics for the two upcoming work programmes for Horizon Europe (priorities mapped to **Research** & **Innovation** in Table 3) and Digital Europe (priorities mapped to **Deployment** in Table 3), and to identify in which objectives of the work programmes the priorities could be covered across a timeline, to also facilitate the transfer of technologies between core research and applied research.

Based on the analysis in Section 5.2, currently and past running projects, we also identified a timeline for vertical pilots (from Research to Deployment) in different sectors.

Table 3 presents the result of mapping R&I&D priorities to work programmes and topics, while Table 4 maps vertical pilots.

Table 3. Mapping R&I&D priorities to work programmes and topics.

	Work programme		
Priority	**2021-2022**	**2023-2024**	**2025-2027**
R1.1 - Low-cost, high-volume connectivity	Instrument: Research Topic: 5G	Instrument: Research Topic: 5G	Instrument: Innovation Topic: 5G and IoT
R1.2 - Low-power connectivity schemes	Instrument: Research Topic: 5G	Instrument: Innovation Topic: 5G and IoT	Instrument: Deployment Topic: IoT
R2.1 Novel data processing architectures	Instrument: Research Topic: DM and IoT	Instrument: Research Topic: DM and IoT	Instrument: Innovation Topic: DM and IoT
R2.2 IoT data processing optimised micro processing units	Instrument: Research Topic: IoT and CPS	Instrument: Innovation Topic: IoT and CPS	Instrument: Deployment Topic: IoT
R2.3 Highly scalable and low latency ledgers for IoT	Instrument: Research Topic: IoT and DL	Instrument: Innovation Topic: IoT and DL	Instrument: Deployment Topic: IoT and DL
R3.1 Novel future proof cybersecurity	Instrument: Research Topic: CS and AI	Instrument: Research Topic: CS and AI	Instrument: Research Topic: IoT
R3.2 IoT data traceability and trust	Instrument: Innovation Topic: IoT and DL	Instrument: Deployment Topic: IoT and DL	
R4.1 IoT data dictionaries deployed at scale	Instrument: Deployment Topic: IoT	Instrument: Deployment Topic: IoT	
R4.2 Semi-automated data interoperability	Instrument: Research Topic: AI and DM	Instrument: Research Topic: AI, DM and IoT	Instrument: Innovation Topic: AI, DM and IoT
R4.3 Semi-automated process interoperability		Instrument: Research Topic: AI and DM	Instrument: Research Topic: AI, DM and IoT

	Work programme		
Priority	**2021-2022**	**2023-2024**	**2025-2027**
R5.1 Privacy-by-design for IoT devices	Instrument: Research Topic: IoT, CPS and CS	Instrument: Innovation Topic: IoT, CPS and CS	Instrument: Deployment Topic: IoT, CPS and CS
R5.2 Security & Privacy-by-design for IoT services	Instrument: Deployment Topic: IoT, CPS and CS	Instrument: Deployment Topic: IoT, CPS and CS	
R6.1 Dynamic orchestration of decentralised AI pipelines	Instrument: Research Topic: CC and AI	Instrument: Research Topic: CC, AI and IoT	Instrument: Innovation Topic: CC, AI and IoT
R6.2 Native AI-capable devices	Instrument: Research Topic: CPS and AI	Instrument: Research Topic: CPS, AI and IoT	Instrument: Deployment Topic: CPS, AI and IoT
R6.3 AI for Humans: understandable and ethical decisions	Instrument: Research Topic: AI	Instrument: Research Topic: AI	Instrument: Innovation Topic: AI and IoT
R6.4 Validated AI algorithms for IoT use cases	Instrument: Innovation Topic: AI and IoT	Instrument: Deployment Topic: AI and IoT	Instrument: Deployment Topic: AI and IoT
R7.1 Large IoT & digital infrastructures	Instrument: Deployment Topic: IoT	Instrument: Deployment Topic: IoT	
R7.2 Semi-autonomous IoT infrastructures	Instrument: Research Topic: IoT and CC	Instrument: Innovation Topic: IoT and CC	Instrument: Deployment Topic: IoT and CC
R7.3 Autonomous IoT infrastructures		Instrument: Research Topic: IoT and CC	Instrument: Research Topic: IoT and CC
R8.1 Sustainable IoT by design	Instrument: Research Topic: IoT	Instrument: Innovation Topic: IoT	Instrument: Deployment Topic: IoT
R8.2 Augmented IoT	Instrument: Innovation Topic: IoT and HCI	Instrument: Deployment Topic: IoT and HCI	

	Work programme		
Priority	**2021-2022**	**2023-2024**	**2025-2027**
R8.3 Tactile Internet	Instrument: Innovation Topic: 5G, IoT and HCI	Instrument: Deployment Topic: 5G, IoT and HCI	
R8.4 IoT for sustainability	Instrument: Deployment Topic: IoT	Instrument: Deployment Topic: IoT	Instrument: Deployment Topic: IoT
R9.1 IoT data market architectures	Instrument: Innovation Topic: DL, DM and IoT	Instrument: Innovation Topic: DL, DM and IoT	
R9.2 Novel business models to incentivise data sharing	Instrument: Research Topic: IoT and DM	Instrument: Innovation Topic: IoT and DM	
R9.3 Large data marketplaces for IoT scenarios		Instrument: Deployment Topic: IoT, DL and DM	Instrument: Deployment Topic: IoT, DL and DM
R10.1 Energy (semi)-autonomous devices	Instrument: Research Topic: IoT and CPS	Instrument: Research Topic: IoT and CPS	Instrument: Innovation Topic: IoT and CPS
R10.2 Bio-compatible sensors	Instrument: Research Topic: IoT and CPS	Instrument: Research Topic: IoT and CPS	Instrument: Innovation Topic: IoT and CPS

Table 4. Mapping vertical pilot priorities to work programmes and topics.

	Work programme		
Priority	**2021-2022**	**2023-2024**	**2025-2027**
V1. Agriculture	Instrument: Deployment	Instrument: Deployment	
V2. Smart Cities	Instrument: Deployment	Instrument: Deployment	
V3. Healthcare	Instrument: Deployment	Instrument: Deployment	

	Work programme		
Priority	**2021-2022**	**2023-2024**	**2025-2027**
V4. Manufacturing	Instrument: Deployment	Instrument: Deployment	
V5. Energy Management	Instrument: Innovation	Instrument: Deployment	
V6. Insurance	Instrument: Innovation	Instrument: Deployment	
V7. Media	Instrument: Research	Instrument: Innovation	Instrument: Deployment
V8. Transportation	Instrument: Research	Instrument: Innovation	Instrument: Innovation
V9. Safety & Defence	Instrument: Research	Instrument: Innovation	Instrument: Deployment

6 STRATEGY BOARD STRUCTURAL RECOMMENDATIONS

6.1 Strategy Board Approach

In this context of WP1 activities lead by MI, NGIoT organised two workshops in Switzerland to explore ways to enhance the cooperation and coordination among IoT related fora and organisations across Europe in order to consolidate the European IoT ecosystem.

On March 3rd 2020, NGIoT organised a *"Workshop on European Research Support and Contribution to Global Standardisation, Internet of Things Perspectives"* at the International Telecommunication Union (ITU) in Geneva. The event gathered European and international experts in the field of standardisation, as well as members of the public administration, private sector, and academia, and explored possible paths to foster collaboration between IoT research and global IoT standardisation.

Moreover, as part of the activities organised in the framework of WP1, NGIoT hosted a *"Workshop on Value Claiming"* from 4-6 March, 2020 in the Alpine village of Crans Montana in Switzerland. Over the course of three days, NGIoT partners and NGIoT Strategy Board members actively brainstormed and deliberated on the measures to maximise the economic and societal impact of European research on IoT for European industry and citizens.

6.2 Recommendations of the Strategy Board

As a result of the two workshops, multiple e-meetings and interactions with the Strategy Bord, complemented by further research conducted in the scope of WP1, the following 10 recommendations have been identified. The recommendations provides insights on how the instruments in the upcoming work programme may increase market impact of future IoT research outcomes. More in-depth detail is provided in the D1.1 'Ecosystem Building Vision and Report'.

- **SB1:** We recommend enhancing IPR and marketing support for future European research projects on IoT, by providing complementary funding for covering IPR protection costs related to IoT research and innovation results.
- **SB2:** We recommend enhancing the cooperation among all IoT related organisations and fora in order to maximise the synergies among them and to reduce the fragmentation of the European IoT community.
- **SB3:** The IoT Market will be shaped by global standards. In order to maximise the direct impact of the standardisation work at an international level and also to reduce the time-to-market of a standard, we encourage the next European research programme on IoT to encourage direct contribution to global standardisation processes led by global SDOs such as IEEE, IETF, ITU, ISO, IEC, 3GPP and TM Forum.
- **SB4:** We recommend that the next research programme on IoT encourage research projects to apply for patents. The programme could also request that patents, if not exploited by the applicant, should be licensed to European industries within a delay of 12 months.
- **SB5:** We recommend that the next research programme on IoT provides dedicated financial and technical support with experts made freely available to help researchers in redacting and filling patents to protect IoT research and development results financed by the EC.
- **SB6:** We recommend that the European Union provides competitive conditions for IPR by requesting the European Patent Office to exonerate researchers from European research projects and from the academy with regards to patent application and search fees.

- **SB7:** We recommend increasing the impact of the next research programme on IoT by adapting the process for reducing the time-to-market from research project application to marketable products and services.
- **SB8:** We recommend increasing the focus of the calls on IoT in order to adapt to needs, to create more momentum and stimulate a global and dynamic approach.
- **SB9:** We recommend involving an evaluator in the mid-term review of a research project to assess its exploitation potential and provide guidelines and orientations on possible funding.
- **SB10:** We encourage a post-project assessment, one year after the end of the project, to follow up on its results and its impact.

7 CONCLUSIONS AND FUTURE STEPS

This section summarize the current version of the roadmap into recommendations for Horizon Europe and Digital Europe based on the analysis presented in the previous section. The following figure presents the outcomes of the analysis, mapping them to the key ICT areas covered in Horizon Europe and Digital Europe.

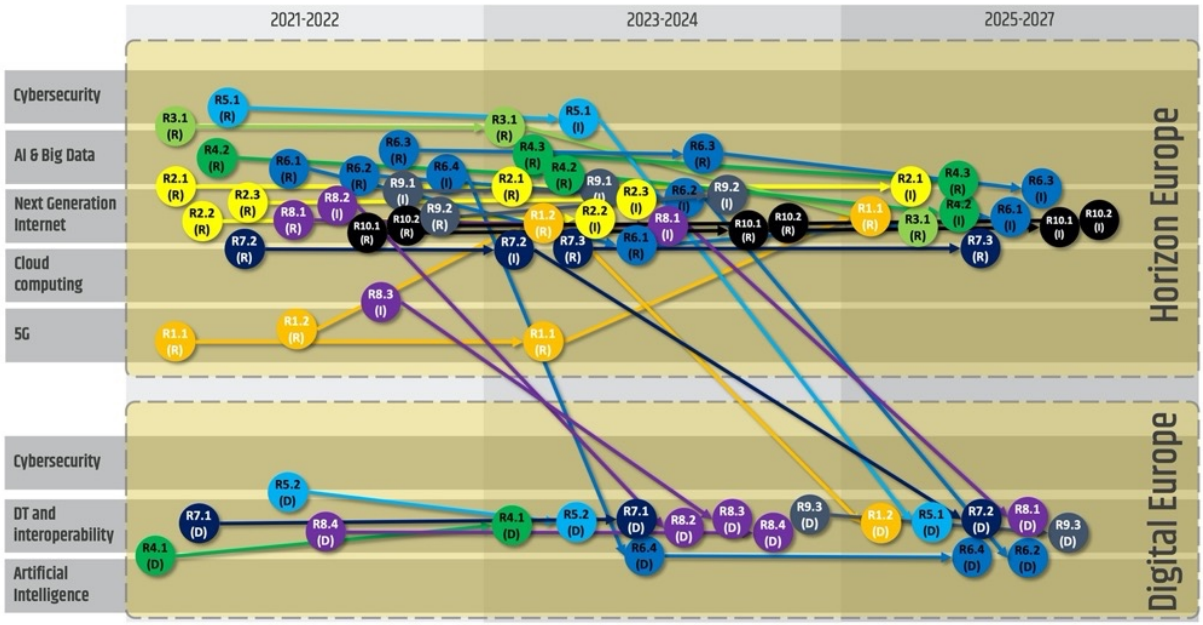


Figure 15. R&I&D priorities timeline, relations and their mapping to work programme topics.

7.1 Key recommendations for 2021-2022

7.1.1 Recommendations for the Horizon Europe programme

- Sustain activities around data value in the relevant work programmes, **increasing focus on IoT generated data** covering architectures (R9.1 - IA) and business models (R9.2 - RIA) **and** boost research on **novel solutions for data processing** using IoT as a primary data source, **both at the software** (R2.1 - RIA) **and hardware stacks** (R2.2 - RIA). These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

- Foster research in the Future Network area that will ensure the development of **reliable, low-cost and scalable IoT networks** (R1.1 - RIA) and **reduce energy impact of IoT networks** (R1.2 / R10.1 - RIA).

- Focus on the **transition from data management to insight generation from data** by delivering ready-to-use AI algorithms in different scenarios (R6.4 - IA) and on the increase of automation **to reduce the cost of the management of complex IoT platforms** and networks focusing on semi-automatic approaches as a first step (R7.2 - RIA / R4.2 - RIA).

- **Leverage the advancements in Artificial Intelligence, Ledgers and other technologies** to evolve IoT platforms beyond today's limitations by introducing dynamic orchestration of AI processes

(R6.1 - RIA), making AI decisions human understandable (R6.3 - RIA), increasing scalability and reducing latency of distributed ledgers (R2.3 - RIA).

- Prioritise the research on **machine-human** interaction in the IoT arena **following a multidisciplinary approach** by scouting solutions for augmented reality and digital twins (R8.2 - IA), tactile internet (R8.3 - IA), while targeting a sustainable IoT by design (R8.1 - RIA).

- **Support the establishment of large IoT trials in new domains** beyond the ones covered today by the IoT Large Scale Pilots[151] (LSPs), such as Energy Management, Insurance (IA) and Media, Transportation, and Safety & Defence (RIA). These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

- **Develop security-by-design and privacy-by-design IoT architectures and technologies** (R5.2 - RIA) capable of dealing with future threats (R3.1 - RIA) and increasing traceability and trust of IoT generated data (R3.2 - IA).

- Develop **IoT miniaturisation** (R2.2 - RIA, R6.2 - RIA), **energy harvesting** (R10.1 - RIA) **and pervasiveness** while **ensuring the environment compatibility** (R10.2 - RIA) of this new generation of devices.

7.1.2 Recommendations for the Digital Europe programme

- Support initiatives aimed at **increasing trust in IoT adoption through cybersecurity and privacy-by-design (GDPR compliance), as well as those seeking a better understanding of ethics and privacy** implications by deploying at large scale state-of-the art solutions for IoT services cyber-security (R5.2). These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

- **Facilitate access to large computational facilities needed to harness the complexity of analysing terabytes** (or petabytes) of IoT generated data and ensure sovereignty by deploying large scale (federated) digital infrastructures across Europe (R7.1). These activities are instrumental for the realisation of EU Data Spaces and Federated Clouds as envisioned in the EU Data Strategy.

- Sustain the **development and uptake of cross-domain harmonised data models**, following the path established by OASC[152], to **increase IoT application interoperability and replicability** especially in the public sector across Europe (R4.1), fostering them as requirements in related public procurements. These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

- **Transfer the experience matured by running LSPs** in the sectors of Smart Cities, Agriculture and Healthcare to a wider set of actors **through joined innovation procurement** and similar actions. These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

[151] https://european-iot-pilots.eu/

[152] OASC, the Open & Agile Smart Cities network, strives to establish the Minimum Interoperability Mechanisms (MIMs) needed to create a smart city market. See https://oascities.org/about-oasc/

- **Deploy secure and highly scalable IoT and digital infrastructures** (R7.1) with special focus on edge capacity, leveraging on global networking technologies such as IPv6 and 5G. These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

- **Leverage the potential of IoT for sustainable development**, in line with the UN Sustainable Development Goals (SDGs) (R8.4).

- **Contribute to the technological independence and autonomy of Europe in terms of IoT critical infrastructures and services** by increasing the scale of IoT infrastructure available to EU citizens (R7.1) leveraging common and free access to data standards (R4.1) and providing secure-by-design IoT services (R5.2).

7.2 Key recommendations for 2023-2024

7.2.1 Recommendations for the Horizon Europe programme

- Sustain activities around data value in the relevant work programmes, **increasing focus on IoT generated data** covering architectures (R9.1 - RIA) and business models (R9.2 - IA) **and** boost research on **novel solutions for data processing** using IoT as a primary data source, **both at the software** (R2.1 - RIA) **and hardware stacks** (R2.2 - IA). These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

- Foster research in the Future Network area that will ensure the development of **reliable, low-cost and scalable IoT networks** (R1.1 - RIA) and **reduce energy impact of IoT networks** (R1.2 - IA / R10.1 - RIA).

- Focus on the increase of automation **to reduce the cost of the management of complex IoT platforms** and networks applying at scale semi-automatic approaches (R7.2 - IA) and automatic ones (R7.3 - RIA) to govern IoT infrastructures, while researching semi-automatic approaches for data (R4.2 - RIA), and process interoperability (R4.3 - RIA).

- **Leverage the advancements in Artificial Intelligence, Ledgers and other technologies** to evolve IoT platforms beyond today's limitations by introducing dynamic orchestration of AI processes (R6.1 - RIA), increasing scalability and reducing latency of distributed ledgers (R2.3 - RIA).

- Prioritise the research on **machine-human** interaction in the IoT arena **following a multidisciplinary approach** by targeting a sustainable IoT by design (R8.1 - IA).

- **Support the establishment of large IoT trials in new domains** beyond the ones covered today by IoT LSPs, such as Media, Transportation, and Safety & Defence (IA). These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

- **Develop security-by-design and privacy-by-design IoT architectures and technologies** (R5.2 - IA) capable of dealing with future threats (R3.1 - RIA).

- Develop **IoT miniaturisation** (R2.2 - IA, R6.2 - IA), **energy harvesting** (R10.1 - RIA) **and pervasiveness** while **ensuring the environment compatibility** (R10.2 - RIA) of this new generation of devices.

7.2.2 Recommendations for the Digital Europe programme

- Support initiatives aimed at **increasing trust in IoT adoption through cybersecurity and privacy-by-design (GDPR compliance), as well as those seeking a better understanding of ethics and privacy** implications by deploying at large scale state-of-the art solutions for IoT services cyber-security (R5.2).

- **Facilitate access to large computational facilities needed to harness the complexity of analysing terabytes** (or petabytes) of IoT generated data and ensure sovereignty by deploying large scale (federated) digital infrastructures across Europe (R7.1). These activities are instrumental for the realisation of EU Data Spaces and Federated Clouds as envisioned in the EU Data Strategy.

- Sustain the **development and uptake of cross-domain harmonised data models**, following the path established by OASC, to **increase IoT application interoperability and replicability** especially in the public sector across Europe (R4.1). These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

- **Transfer the experience matured by running LSPs** in the sectors of Smart Cities, Agriculture, Healthcare, Manufacturing, Energy Management and Insurance to a wider set of actors **through Innovation Procurement** and similar actions. These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

- **Deploy secure and highly scalable IoT and digital infrastructures** (R7.1, R8.2, R8.3, R9.3) with special focus on edge capacity and ability to create large IoT markets for augmented and tactile internet, leveraging on global networking technologies such as IPv6 and 5G. These activities are instrumental for the realisation of EU Data Spaces and Federated Clouds as envisioned in the EU Data Strategy.

- **Leverage the potential of IoT for sustainable development**, in line with the UN Sustainable Development Goals (SDGs) (R8.4).

- **Contribute to the technological independence and autonomy of Europe in terms of IoT critical infrastructures and services** (R7.1, R4.1, R5.2).

7.2.3 Key recommendations for 2025-2027

7.2.3.1 Recommendations for the Horizon Europe programme

- Boost exploration of **novel solutions for data processing** (R2.1 - IA).

- Foster initial deployments and experimentation of **reliable, low-cost and scalable IoT networks** (R1.1 - IA).

- Focus on the increase of automation **to reduce the cost of the management of complex IoT platforms** and networks researching automatic approaches to govern IoT infrastructures (R7.3 - RIA) and semi-automatic approaches for process interoperability (R4.3 - RIA).

- **Leverage the advancements in Artificial Intelligence** to evolve IoT platforms by introducing dynamic orchestration of AI processes at large scale (R6.1 - IA).

- **Develop security-by-design and privacy-by-design IoT architectures and technologies** capable of dealing with future threats (R3.1 - RIA).

- Promote the large scale testing of **sustainable** (R10.1 - IA) **and biocompatible IoT devices** (R10.2 - IA).

7.2.3.2 Recommendations for the Digital Europe programme

- Support initiatives aimed at **increasing trust in IoT adoption through cybersecurity and privacy-by-design (GDPR compliance), as well as those seeking a better understanding of ethics and privacy** implications by deploying at large scale state-of-the art solutions for IoT devices cyber-security (R5.1).

- **Transfer the experience matured by running LSPs** in the sectors of Media, Transportation, Safety & Defence to a wider set of actors **through Innovation Procurement** and similar actions. These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

- **Support the creation of a set of open and royalty-free-to-use trustable classification and prediction algorithms covering key sectors of the European economy (R6.4)**. These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

- **Deploy sustainable and highly scalable IoT and digital infrastructures** (R8.1, R9.3) with special focus on creation of large scale data markets. These activities are instrumental for the realisation of EU Data Spaces and Federated Clouds as envisioned in the EU Data Strategy.

- **Leverage the potential of IoT for sustainable development**, in line with the UN Sustainable Development Goals (SDGs) (R8.4).

- **Contribute to the technological independence and autonomy of Europe in terms of IoT critical infrastructures and services** (R7.1, R4.1, R5.2).

7.3 General Recommendation of cohesive approaches

A large number of topics are highlighted as cross-cutting topics among key research areas including: Cloud, IoT and Big Data. To facilitate the cross-adoption between these research areas, a well orchestrated and focused programme may be beneficial and speed up the research development and early take up of outcomes.

In this sense, as already highlighted in the NGIoT Scoping Paper, such a cohesive approach may be pursued by the establishment of a transversal partnership among Cloud, IoT and Big Data stakeholders, both private and public, within Horizon Europe.

The aim of such a public-private partnership (PPP) should be to unleash Europe's potential to ***deliver large scale digital infrastructures serving the needs and purposes of Europe's economy and society, in line with the key goals of the EU policy framework: empowering people with a new generation of technologies; supporting European strategic autonomy; guaranteeing and protecting EU civil rights (digital or not); and ensuring the sustainability of the EU economy***.

Based on the analysis summarised in the table, we recommend the following priorities to be explored in such a PPP:

- Support solutions to ***drastically reduce costs of deployment and management of large digital infrastructures***, spanning from the devices at the edge through the network (R1.1) up to data

centres (R7.2 / R7.3).

- Ensure that ***large digital infrastructures have a reduced environmental impact*** (R1.2 / R10.2) and ***target sustainability*** (R8.1 / R10.1), while dynamically and opportunistically scaling up (by connecting resources where and when needed).

- Evolve data processing (R2.1, R2.3), management (R4.2, R4.3) and machine learning solutions (R6.1) to ***enable the next generation of IoT platforms (R8.3) and data markets around them*** *(R9.1)* ***thanks to the novel capacities offered by cutting edge solutions for network and cloud***.

- Apply outcomes to use case scenarios that ***put European societal values at the centre*** (R6.3 / R8.1) ***and promote a positive vision of Europe's digital future***.

7.4 Future steps

The current version of the "IoT research, innovation and deployment priorities in the EU" white paper provides a solid base for discussion with IoT stakeholders and actors contributing to the developed of related key enabling technologies. NGIOT in the next period will focus on engaging additional stakeholders beyond the Advisory Board to refine the priorities, their timeline and hence the reccomendations to the European Commission for the upcoming work programmes.

The engagement of the stakeholders coordinated by WP4 and T3.2 will occur trough different means, ranging from workshops and webinars to one-to-one interviews and discussions.

Content of the "IoT research, innovation and deployment priorities in the EU" white paper will be leveraged to provide feedback to relevant EC consultations.

8 REFERENCES

NGIOT. Description of Action (2018)

NGIOT. D1.1 - Ecosystem Building Vision and Report (2020)

NGIOT. D3.2 - Future Trends in IoT (2020)

NGIOT. Building a roadmap for the Next Generation Internet. Research, innovation and implementation 2021 – 2027 (2019)

AENEAS, ARTEMIS-IA and EPoSS. ECS Strategic Research Agenda 2020 (2020)

AIOTI, Research and Innovation Priorities for IoT, 2018.

AIOTI. IoT data marketplaces for the agri-food sector: a first look to use cases for smart farming and across the food chain (2020)

AIOTI. IoT Relation and Impact on 5G (2019)

Ashton, Kevin. That 'internet of things' thing. RFID journal 22.7 (2009)

Bain & company. Europeans Extend Their Lead in the Industrial Internet of Things (2018)

Bauer, Martin, et al. IoT reference architecture. Enabling Things to Talk. Springer, Berlin, Heidelberg (2013). 163-211

CBI. The European market potential for integrated internet of things and big data services (2020)

CEMA. Full deployment of agricultural machinery data-sharing: technical challenges & solutions (2020)

Chesbrough Henry and Vanhaverbeke Wim. Open Innovation and Public Policy in the EU with Implications for SMEs (2018).

Control Engineering. 2020 System Integrator Giants (2020)

Deloitte. The fourt Industrial Revolution (2020)

DIGITAL SME. DIGITAL SME input on the EC's White Paper on Artificial Intelligence (AI) (2020)

EC. Cross-cutting activities work programme 2016-2017 (2016)

EC. A Digital Single Market Strategy for Europe (2015)

EC. Advancing the Internet of Things in Europe (2016)

EC. Digitisation Research and Innovation - Transforming European Industry and Services (2017)

EC. Digitising European Industry - Reaping the full benefits of a Digital Single Market (2016)

EC. Horizon Europe: the next EU research & innovation investment programme (2021 – 2027) (2019)

EC. ICT work programme 2018-2020 (2018)

EC. Shaping the Europe's digital future (2020)

EC. The European AI Landscape (2018)

EETimes. European Consortium to Develop Standard Edge Computing Platform (2019)

EIP-SCC. European Context (2020)

EPSC. Rethinking strategic autonomy in the digital age (2019)

Ericsson. Edge computing and deployment strategies for communication service providers (2020)

European Cyber Security Organisation (ECSO). Strategic Research and Innovation Agenda (2016)

Future Cities Catapult. IoT investment case toolkit: smart parking (2016)

Garnter. Magic Quadrant for Industrial IoT Platforms (2019)

Gartner. Hype Cycle for the Internet of Things (2019)

HUB4NGI. NGI Guide v3 (2019)

I-Scoop. Edge computing: the what, how and where of the edge (2020)

IDC. Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination (2014)

IDC. The Technology Impacts of Edge Computing in Europe (2019)

Internet Society. IoT Trust by Design (2018)

IoT Analystics. IoT Investments 2018 (2018)

IoT Analytics. 40 emerging IoT technologies you should have in your radar (2019)

IoT4Industry. SME Barriers and opportunities for adopting IoT (2018)

ISO. IoT Reference Architecture, ISO/IEC CD 30141 (2018)

ITU. Architectural reference models of devices for Internet of things applications. ITU Recommendation ITU-T Y.4460 (2019)

ITU. Overview of the Internet of things. ITU Recommendation ITU-T Y.2060 (2012)

Kearney. Rebooting Europe‘s high-tech industry (2013)

KPMG. Converging 5G and IoT: a faster path to smart manufacturing (2019)

Lin, Shi-Wan, et al. The industrial internet of things volume G1: reference architecture. Industrial Internet Consortium (2017): 10-46.

LSP. IoT Pilots Architectures (2020)

LSP. The European Large-Scale Pilots Programme - Driving IoT Innovation at Scale in Europe (2019)

MESTECC. National Internet of Things (IoT) Strategic Roadmap (2014)

Michiel Leenaars et al. Next Generation Internet 2025 (2018)

Minerva, Roberto, Abyi Biru, and Domenico Rotondi. "Towards a definition of the Internet of Things (IoT)." IEEE Internet Initiative 1.1 (2015): 1-86.

Mohammad Jamshidi, Systems of Systems Engineering: Principles and Applications (2009)

NGI. NGI, For an Internet of Humans (2019)

NSTF. National Integrated Information and Communication Technology (ICT) Policy White Paper (2016)

Open Access Government. The cybersecurity challenges of 5G and IoT (2020)

Petar Popovski, “The Supernatural Touch of Tactile Internet, Big Data, AI, and Blockchain”, 2018.

Plattform Industrie 4.0. “Reference Architectural Model Industrie 4.0 (RAMI4.0) - An Introduction” (2018)

ProMéxico. Crafting the Future: A Roadmap for Industry 4.0 In Mexico (2016)

Reporter Link. Europe 5G in IoT Market to 2027 - Regional Analysis and Forecasts by Radio Technology; Device Range; End-User Industry (2019)

Roland Berger. Artificial Intelligence – A strategy for European startups (2018)

Selamat et al. Big Data and IoT Opportunities for Small and Medium-Sized Enterprises (SMEs) (2019)

Smart Industry. IoT Readiness: Is Europe up to it? (2018)

STL Partners. AWS, Azure & Google at the edge: How much fit is telco edge computing? (2017)

Strategic Council for AI Technology. Artificial Intelligence Technology Strategy (2017)

SynchroniCity. Reference Architecture for IoT Enabled Smart Cities - D2.10 (2018)

SynchroniCity. A guide to SynchroniCity (2020)

Ullrich A. and Vladova G. Weighing the Pros and Cons of Engaging in Open Innovation. Technology Innovation Management Review, 6(4): 34-40 (2016).

Vodaone. A new IoT regulátory framework for Europe (2019)

WSO2. A reference architecture for the Internet of Things (2016)

ANNEX I

Grant Agreement N°: 825082

Call: H2020-ICT-2018-2

Topic: ICT-27-2018-2020, Internet of Things

Type of action: CSA

Next Generation Internet of Things

Deliverable number	NA
Deliverable title	Market Research and Business Modelling
WP number	WP3
Lead beneficiary	AS
Deliverable type	Report
Dissemination level	
Delivery due month	
Actual submission month	
Authors	Francisco Molina, Gabriela Hrasko, Olivia Döll
Internal reviewers	
Document version	V6
Project start date	01.11.2018
Project end date	31.10.2021
Duration in months	36 months

Important Notice: Working Document

This Market Research and Business Modelling report is intended to support the development of the research and innovation strategy roadmap in Work Package 3 (WP3) by providing initial input with regards to market challenges and opportunities associated with IoT applications. This Market Research and Business Modelling report is led by Archimede Solutions (AS) and is part of Task 1 of WP3, whose objective is to provide a clear picture on current obstacles, as well as opportunities, that IoT related activities encounter and offer. As a way to enhance Europe competitiveness in the global market for IoT products, the Market Research and Business Modelling report will focus on identifying the priorities and opportunities in IoT based on industry-needs. This deliverable is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 825082.

1. EXECUTIVE SUMMARY

The Market Research and Business Modelling report is developed with the objective to provide an in-depth analysis of the IoT market, IoT application domains, IoT-related emerging business models and technology drivers to help identify economic opportunities and challenges related to the research, development and implementation of IoT-related activities. The focus of the report is to align with the priorities and industry-needs, in order to serve as an input for the NGIOT Roadmap to enhance Europe competitiveness in the global market for IoT products.

Section 3 describes the economic outlook and potential of IoT on a industry segment and region specific levels, showing different ranges of very positive scenarios that go from $1.1 Trillion to over $3 Trillion with CAGRs from around 17% to over 30% depending on each of the study's assumptions and methodologies. Section 4 elaborates on the NGIOT Scoping paper survey results of industry domains and priorities and describes the Value Chain withing these industries. Section 5 describes the technology drivers influencing IoT, including Edge/Cloud computing, 5G, Artificial Intelligence, Augmented Reality, Digital Twin, and Distributed Ledgers. Section 6 presents different and innovative business models with worldwide examples related to IoT. And section 7 gets insights from these previous sections to draw an European Internet of Things landscape and derive the challenges and opportunities in the following chapters.

Five general opportunities and specific industry domain opportunities were identified together with 12 economical challenges, 9 research challenges and industry domain specific challenges described in sections 8 and 9. Based on these challenges and opportunities, 18 high-level recommendations for the Horizon Europe and Digital Europe programmes were drafted to be further developed in the NGIOT roadmap.

Abbreviations

D	Deliverable
EC	European Commission
WP	Work Package
WT	Work Task

Contents

List of Figures

2. INTRODUCTION

2.1. Context

Nowadays, the Internet is an integral part of our lives and business. We can exploit the opportunities it creates, but we have to be aware and mitigate the risks at the same time. In order to support these activities, Europe aims to re-invent the next generation of the Internet by "shaping a value-centric, human and inclusive Internet for all"[1]. We can name the Next Generation Internet (NGI) initiative launched by the Digital Single Market of the European Commission (EC) in autumn 2016, with the goal to contribute to creating a 'highly adaptive and resilient', 'trustworthy' and 'sustainably open' human-centric Internet.

NGI analyses advanced technologies including, in addition to IoT, privacy and trust, search and discovery, decentralised architectures, blockchain, social media, interactive technologies, as well as technologies supporting multilingualism and accessibility[2]. The program also focuses in the areas of research on artificial intelligence, cloud computing, ultra-reliable connectivity beyond 5G, edge computing, and big data, which are crucial for capturing the opportunities that Internet offers. This wide range of innovative technologies provides a necessary condition for sufficient capabilities enabling successful digital transformation.

With the mission-oriented Horizon Europe and Digital Europe vision, complemented by structural funds and private investments, Europe has laid out the tracks to tackle this complexity, to the benefit of European citizens, and beyond. As the new Commission was announced, the focus on digital and the link to the digital single market was further emphasised, including Commissioner-designate Executive Vice President Margrethe Vestager given the portfolio title "a Europe fit for the Digital Age". This marks not only a level of ambition but also a strategic integrated approach to technology, market creation and competition not seen before. The NGIoT scoping paper, the following NGIoT Market Research and Business Modelling study and the coming Strategy Roadmap should be seen in this light, supporting directly this ambition of the EC.

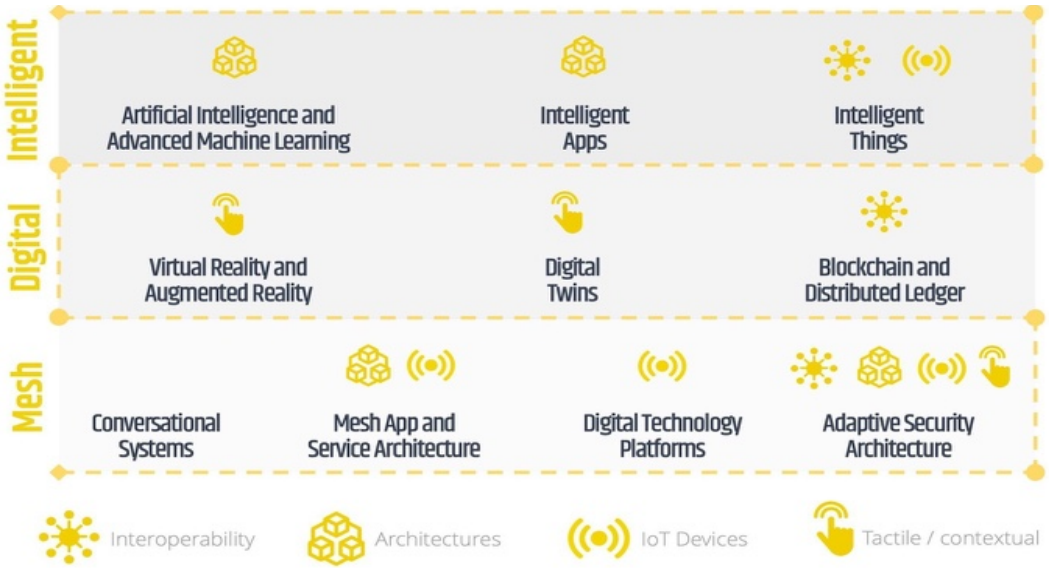


Figure 1. European Research, Innovation and Implementation related to Internet of Things[3]

[1] https://ngi.eu/wp-content/uploads/sites/48/2019/09/NGI-for-an-Internet-of-Humans-1.pdf
[2] https://ec.europa.eu/digital-single-market/en/news/next-generation-internet-brochure
[3] NGIoT Scoping Paper

As outlined by the European Commission, the Internet of Things (IoT) represents the next step of disruptive digital innovation where "any physical and virtual object can be connected to other objects and to the Internet, creating a fabric of connectivity between things and between humans and things"[4]. The Internet of Things is a technology enabler that is central to the successful implementation of the EU Digital Single Market Strategy. Similarly, to cloud computing, big data, artificial intelligence, robotics, machine learning, IoT will contribute to profoundly transforming the EU's economy and society [5].

The strategy for successful implementation and exploitation of IoT in all economic areas is based on three main pillars: a **thriving IoT ecosystem**, a **human-centred IoT** approach and a **single market for IoT**. In March 2015 the Alliance for the Internet of Things[6] (AIOTI) was set with the goal to coordinate ongoing activities and set a direction for the full exploitation of opportunities created by IoT. Given the importance of IoT for the economy, there are many other initiatives created (Horizon 2020 ICT Work Programme 2018-2026, IoT-European Platforms Initiative, IoT Large-Scale Pilots Programme (LSPs)). IoT is regarded as a key component and challenge towards the 'Digitising European Industry' strategy and the Next Generation Internet of Things. Thus, it is a catalyst for the digital revolution, and it brings transformation from the economic, business and societal point of view changing the whole ecosystem. The Internet of Things (IoT) is involved in various highly impactful application domains, ranging from healthcare and agriculture to industry and leisure. Also, the EU invests almost EUR 500 million in IoT-related research, innovation and deployment under Horizon 2020 for the period 2014-2020.

IoT is also crucially tied to advancement in other fields such as cloud computing, AI, Human Machine Interaction (HMI), Big Data and data analytics, Quantum Computing, 5G (Road2CPS Technology and Application Roadmap6). It is the key driver of the Big Data phenomenon due to its ability to connect a variety of smart devices or objects which generates a growing amount of data, according to the Strategic Research and Innovation Agenda (SRIA)[7].

The European Commission has published several strategic documents that are setting priorities for the upcoming Multiannual Financial Framework (MFF), which will span the 2021-2027 period. Of central relevance are: the creation of the Digital Single Market, supporting synergies between transport, digital and energy infrastructure, empowering communities and digital capacity building, the compliancy of emerging technologies with the European General Data Protection Regulation (GDPR), the strong commitment towards sustainable development and the 17 UN Sustainable Development Goals (SDGs) of the 2030 Agenda for Sustainable Development, as well as the commitment to defend European digital autonomy, sovereignty and security[8].

The research and innovation roadmap (task 3.3. of WP3) will provide a guidance for the identification of the key research and innovation topics and how to address them. An integral part of the roadmap are the economic, business and societal topics. This report is intended to provide an input both for the working groups (task 3.2) and for the roadmap (task 3.3).

2.2. Objectives

The Market Research and Business Modelling report is developed with the objective to provide an in-depth analysis of the IoT market, IoT application domains, IoT-related emerging business models and technology drivers as well as economic opportunities and challenges related to the implementation of IoT-related activities. The focus of the report is to align with the priorities and industry-needs, in order to enhance Europe competitiveness in the global market for IoT products.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN
[5] NGIoT Scoping Paper
[6] https://aioti.eu/
[7] http://www.bdva.eu/SRIA
[8] NGIoT Scoping Paper

Particularly, the market analysis will examine the current IoT market situation using some standard metrics for market analysis such as market size, market value, historical market growth and market segmentation. A special focus will be on the future predictions of the market behaviour in order to gain some insight in the most probable future evolution and to be able to anticipate future changes and created opportunities. This will significantly contribute to the goal of supporting competitiveness. Especially, understanding the potential of the enhanced reasoning capabilities and increased computational power for the transformation of business-as-usual activities in relation to IoT is crucial. An important part of the report is the identification of the new capabilities that artificial intelligence, edge and cloud technology, deep semantic interoperability and novel contractual arrangements like Blockchain offer to the industry.

Equipped with the knowledge of the actual market situation, the report will further provide a structured overview of current business models as well as emerging innovative business models integrating IoT across key sectors in the industry. This report will provide a significant input for both the tasks 3.2 and 3.3 of WP3. In particular, task 3.2 will benefit from this report with the identified IoT-related opportunities and obstacles, which will provide substantial topics for the discussion of working groups. Additionally, the NGIoT Strategy Board (WP1) will also benefit from that report. Most importantly, this report will serve as input for the Research and Innovation Roadmap (task 3.3), outlining the specific business needs for future research and innovation. It will also provide support for consensus building among suppliers and users across Europe.

2.3. Methodology

The steps for the creation of this report were organized with the key objective to provide task 3.2 and 3.3 leaders as well as the WP1 (Strategy Board) with valuable insights into the economic and business side of the spread of IoT technologies. This should further enhance their deliverables with the key focus being the Research and Innovation Roadmap. Crucial is to understand the key stakeholders on the IoT market as well as market perceptions and reactions with respect to IoT. An integral part are the new business models. All this contributes to a clear summary of open questions or challenges, which should be addressed by future research.

In order to deliver a meaningful report with the goal to be further used by other NGIoT partners, it is crucial to define what information is needed and to develop an effective methodology to allow the efficient extraction of the target information from plenty of resources. With the perspective to deliver a valuable report in a timely manner and to use optimally the assigned resources, steps were regularly discussed with NGIoT partners. The steps were organized as follows:

1) Set-up: during the kick-off meeting of the NGIoT project, we met the EC representatives as well as the other NGIoT partners, which enabled us to understand the project's objectives as whole and have a clear idea how particular WPs and tasks leaders should collaborate together in order to meet the goals. In the first months, information was exchanged during regular NGIoT teleconferences to monitor the progress and align the partners' activities.
2) Information Gathering: after having defined what information is needed, the next step was to identify relevant sources of information (pre-existing documents, market reports, articles, etc.), check reports and articles from relevant initiatives (IoT LSP, IoT Forum, AIOTI, IoT Security Cluster, OASC etc.) and attend several important IoT events (IoT Week, Marketplace Workshop, Procurement Workshop etc.) in order to stay in the loop and be up to date with the topics discussed as well as to lead dialogues with different stakeholders and gather opinions. Another considerable source of information was the input from a broad community of researchers and innovators via the "IoT Research and Development Survey" run by NGIoT from March to July 2019.
3) Scoping Paper and Feedback: regarding the timeline, we were first engaged in orchestration of the Scoping Paper writing effort, where the information from resources mentioned in 2) had to be implemented. Firstly, this activity enabled us to filter out the most important information and deliver a key message regarding the IoT-related economic opportunities and challenges. Furthermore, we

received insightful feedback on the scoping paper from the EC as well as from the Strategy Board. This was not only implemented in the scoping paper, but also in this report.

4) Analysis Phase: firstly, the key reports were analysed and the outline for this report was created. Having once the topics to be investigated further, we enriched the analysis with the other resources mentioned in 1). This process took several months. Furthermore, the report does not only aim at gathering and presenting information, but also at prioritisation of issues to be addressed further. The priority IoT application domains were identified with the IoT Research and Development survey being a significant guidance. The key economic challenges related to IoT were identified based on stakeholder and expert dialogues at relevant events and market, strategy and research reports. The objective is to aggregate the perspectives from various market analyses in order to identify and extract key research priorities from the economic/industry/business side.

5) Validation Cycle: in the first phase of the validation cycle, a preliminary draft was submitted to the NGIoT partners for comments, as we believe they should co-create this report and thus ensure to get useful input for their work in the future. We then implemented the feedback. The new version is still being polished and it is constantly being improved by new information gathering.

6) Outreach Phase. This report will be distributed to NGIoT partners as an input for their tasks. It will also provide a basis for further discussions, consultations and co-creation processes especially for the Research and Innovation Roadmap.

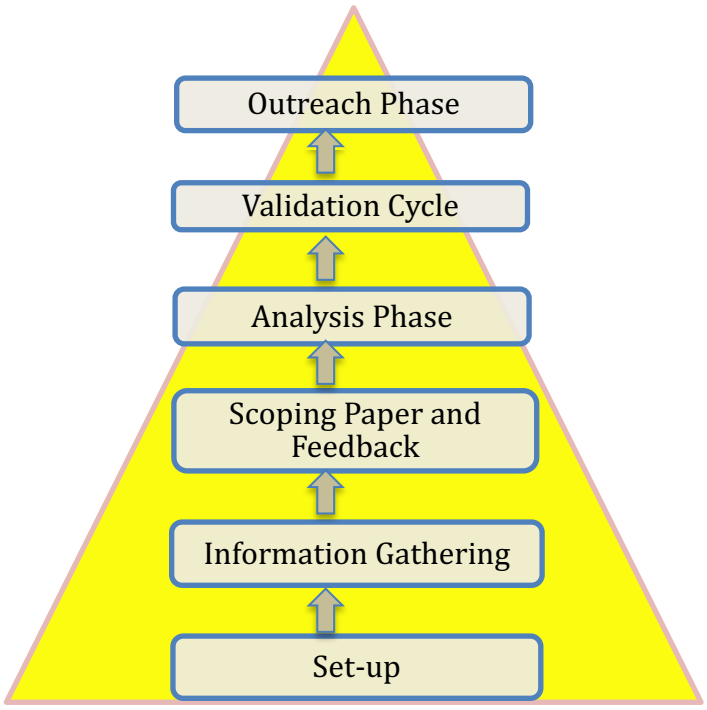


Figure 2. Market Research and Business Modelling report methodology.

3. INTERNET OF THINGS (IOT) GLOBAL MARKET DIMENSIONS, TRENDS AND FORECASTS

This section provides the overview of the basic IoT market metrics as well as the most important IoT market trends. The objective is to provide a picture of the worldwide IoT landscape and its dynamics, and thus, to be able to better understand the IoT market functioning, its opportunities and challenges as well as the unavoidable societal transformation due to IoT.

3.1. IoT Market Overview and Trends

This section is based on the NGIoT Scoping Paper. The reader should be aware that for some of the metrics (e.g. number ot internet connected devices), there are several ways of estimation and we present here projections from several resources. Hence, the numbers are not always the same. The objective is to get an idea of the range where the metrics could be in a particular year.

3.1.1. General Outlook

The current market sentiment and short-term outlook is very positive. Software and platforms are expected to continue to drive the market as more data is moved to the cloud, new IoT applications get brought to market, and analytics continue to gain importance.[9]

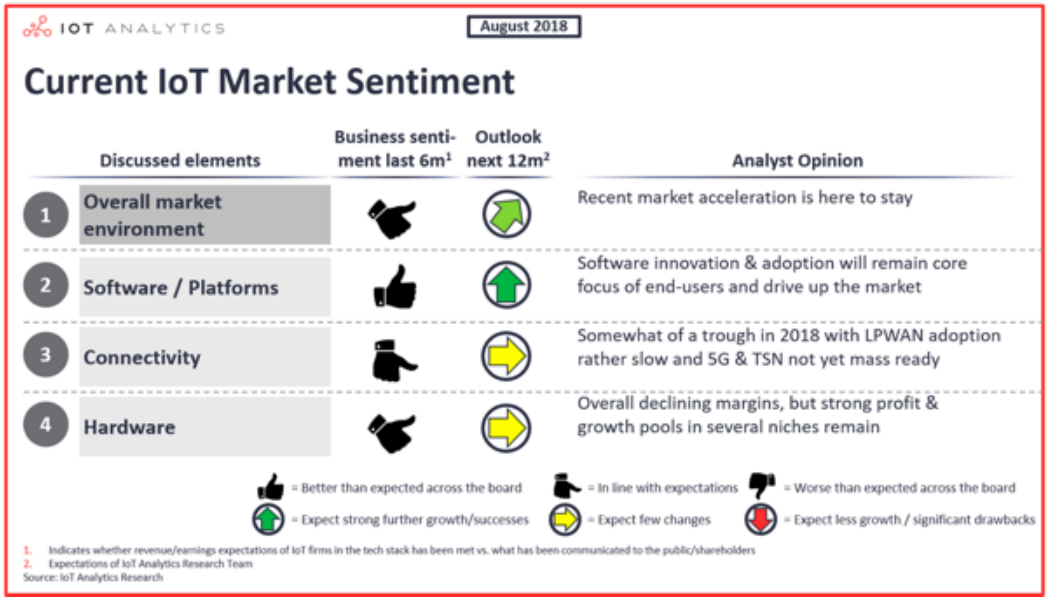


Figure 3. IoT Market Sentiment[10]

"Overall conclusion from 2018 could be summarized as: stable interest, strong overall growth but general economic risks. Cloud and platform firms were especially strong, with some reporting growth rates near 100% for their IoT business. Going forward, the proliferation of new connectivity standards (mostly LPWAN, 5G), the maturation of technologies (platforms, edge, digital twins) and the increased focus on solving customer problems (vs. technical problems) will continue to drive the market. However, the recent global economic slowdown and international trade tensions are expected to somewhat dampen the bright and positive picture of IoT 2018".[11]

[9] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/
[10] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/
[11] https://iot-analytics.com/iot-2018-in-review/

3.1.2. Market Growth

The number of connected devices reached almost 18B in 2018, with IoT devices amounting to 7B. It is predicted that the number of connected devices will almost double and grow to 34B in 2025, which represents about 89 percent growth in seven years. In contrast, the number of IoT connected devices is expected to triple by 2025 to 21.5B[12], as seen in Figure 4. These forecasts illustrate the expected rapid growth of IoT devices in comparison to the growth in the number of generally connected devices.

It is also important to notice that, according to IoT Analytics, the expected growth in IoT devices will be in part "driven by new low-power wide-area (LPWAN) standards as well as 5G" [13]. This number of IoT devices includes all active connections and does not take into consideration devices that were bought in the past but are not used anymore"[14].

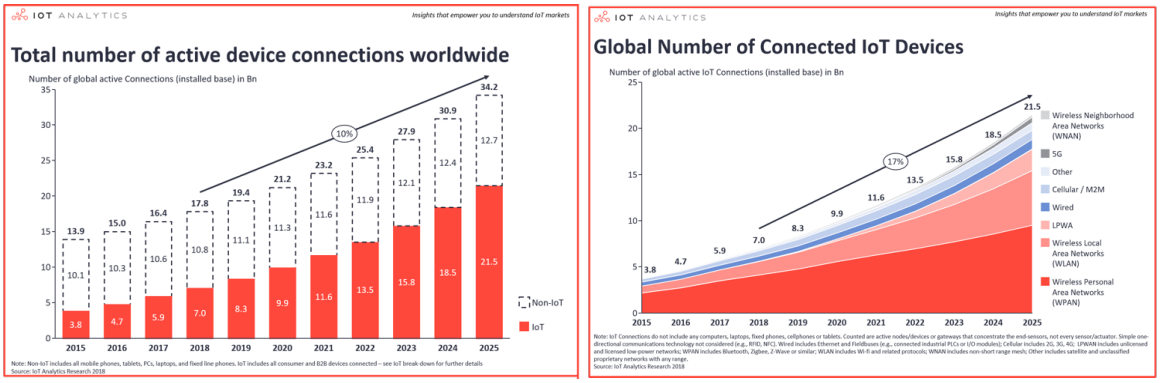


Figure 4. Global active device connections and global connected IoT devices[15]

In order to get a notion of the geographical distribution of this growth, Ericcson´s forecast for cellular IoT connections provides some key insights. Similar to the overall IoT devices projection seen before, the number of devices is expected to more than triple from 2018 to 2025, mostly due to ongoing large-scale deployments in China. The projection is that the number of cellular IoT connections is expected to reach 3.5B in 2023, increasing at a CAGR of 30%, as shown in Figure 5, which also points out that of the 3.5B cellular IoT connections forecast for 2023, North East Asia is anticipated to account for 2.2B[16], claiming around 60% of the total connections. Further geographical analysis corresponds to the next sub-section of this report.

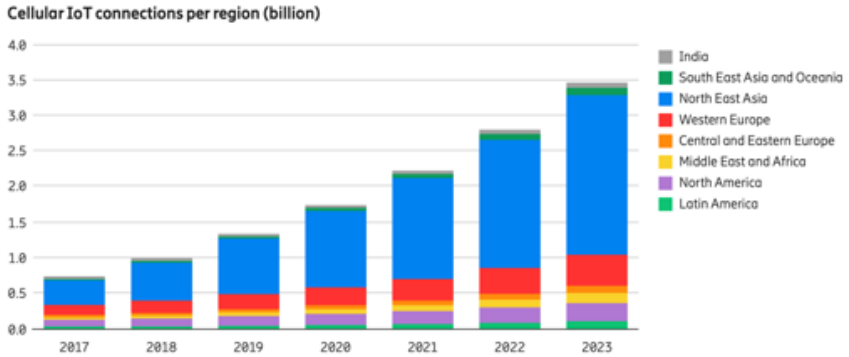


Figure 5. Cellular IoT connections per region[17]

[12] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/
[13] https://iot-analytics.com/iot-2018-in-review/
[14] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/
[15] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/
[16] https://www.ericsson.om/assets/local/mobility-report/documents/2018/ericsson-mobility-report-june-2018.pdf
[17] https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-june-2018.pdf

The IHS Markit predictions, on the other side, shades some light on distribution and growth of IoT within the most important market verticals in the upcoming years. By recognizing the proliferation of IoT devices, sensors and systems as the catalyst of edge-based applications, IHS Markit estimates the number of devices across the key vertical markets shown below in Figure 6, along with their CAGR estimates[18].

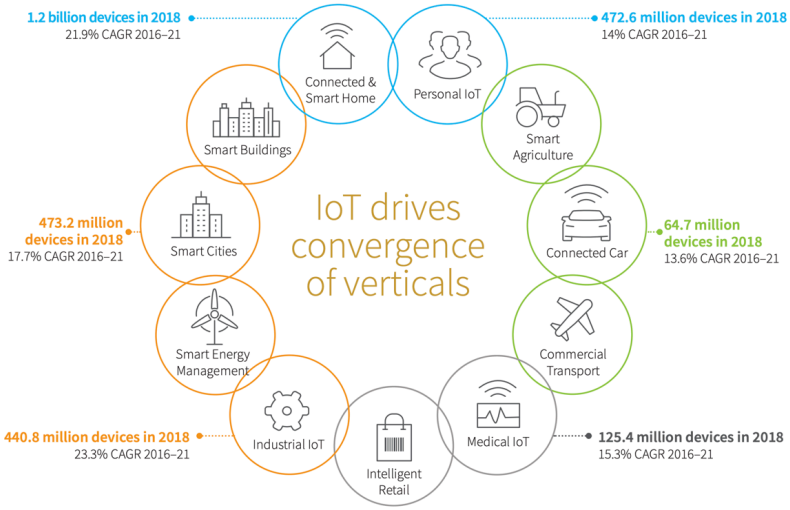


Figure 6. Market Verticals influenced by IoT according to IHS Markit

These 2 notions of geographical and by sector division can be also reflected in the studies made by IoT analytics[19] and the Growth Enabler report[20]. However, these reports state slightly different perceptions, the former giving more importance to connected industry (22%) and smart cities (20%), whereas the latter saying that the global IoT estimated market shares by sub-sector are dominated by smart cities (26%), industrial IoT (24%), medical and healthcare (20%) and smart homes (16%), as shown in shown in Figure 7. Other relevant sub-sectors include connected cars, energy management, wearables, smart utilities and others[21].

Even if the numbers vary from one study to the other because of different approximation methods, it is important to notice that 2 propositions hold true in every study: the first one being that the **main domains are very similar** even if their proportions vary, the second one that **all of the fields are growing rapidly**.

Lastly, it is important to note from the study of IoT Analytics that the main drivers of the industrial adoption of IoT are: IoT-related potential to lower operational costs and risks, increase in productivity and the expansion associated with new products and market segments. Also, that in each of these sectors, thanks to the adoption of IoT technologies, new business models are expected to be developed, including IoT-as-a-service, subscription models, and other asset-sharing models abilitated by the development of new technological capabilities like asset tracking, remote monitoring, preventative maintenance, compliance monitoring, remote diagnostics, etc. These models will be discussed further in this study.

[18] https://cdn.ihs.com/www/pdf/IHS-Markit-2018-Top-Transformative-Technology-Trends.pdf
[19] https://iot-analytics.com/top-10-iot-project-application-areas-q3-2016/
[20] https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf
[21] https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf

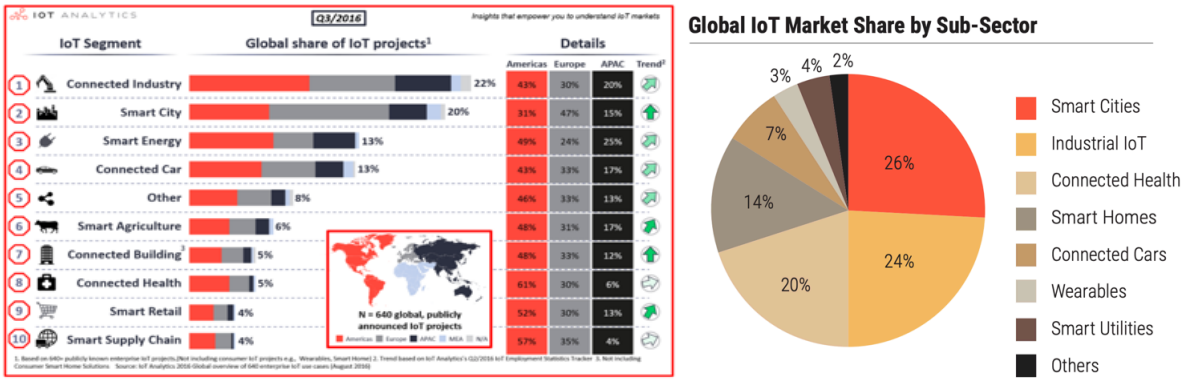


Figure 7. Global share of IoT projects

3.1.3. Market Value

According to IoT analytics, the IoT market value was estimated to amount to $151B in 2018 and a steep growth is predicted with a market value reaching $1,567B in 2025[22], as seen in Figure 8. This significant growth brings many opportunities to exploit IoT technologies. Along with the general term IoT, many technologies have to be further developed and extended to facilitate IoT implementation (e.g. 5G, WLAN, WPAN etc.). The spending on IoT in EMEA with 23 percent of the IoT spending worldwide ranks third in the world, whereas the leader is the APAC region (37 percent) followed by the US (29 percent). However, the growth rate for 2018-2023 is forecasted as being the highest in EMEA (14.3 percent)[23].

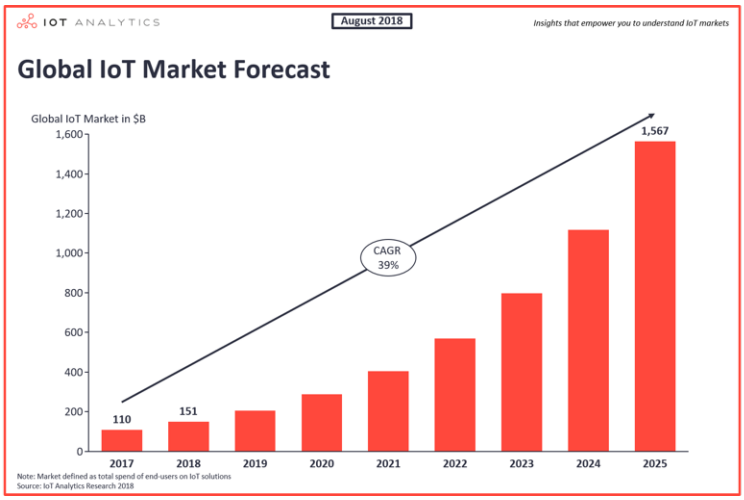


Figure 8. Global IoT Market Value Forecast

Predictions of Bain are that the combined markets of the IoT will grow to about $520B in 2021, which is more than double the $235B spent in 2017. Based on their latest survey of IoT early adopters, Bain is seeing more of their enterprise clients trying out new use cases: 60% in 2018 compared with fewer than 40% in 2016, which is a positive sign. These findings are consistent with many other surveys and early adopter plans that are predicated on analytics, machine learning and AI providing insights that enable successful digital transformation strategies[24].

[22] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/
[23] https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf
[24] https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things/

On a less optimisitic prediction, EY estimates a Global IoT market of US$1.1 Trillion by 2025. Which, in geographical terms, the Asia-Pacific region is forecasted to be the leader in terms of market size 10.9 billion connections by 2025. Followed by North America and Europe with 5.8 billion and 4.9 billion respectively as seen in Figure 9. However, taking into accoung the growth rate, the fastest growing region is Europe and Middle East (EMEA) region with a growth at CAGR of 15.7% through the forecast period[25].

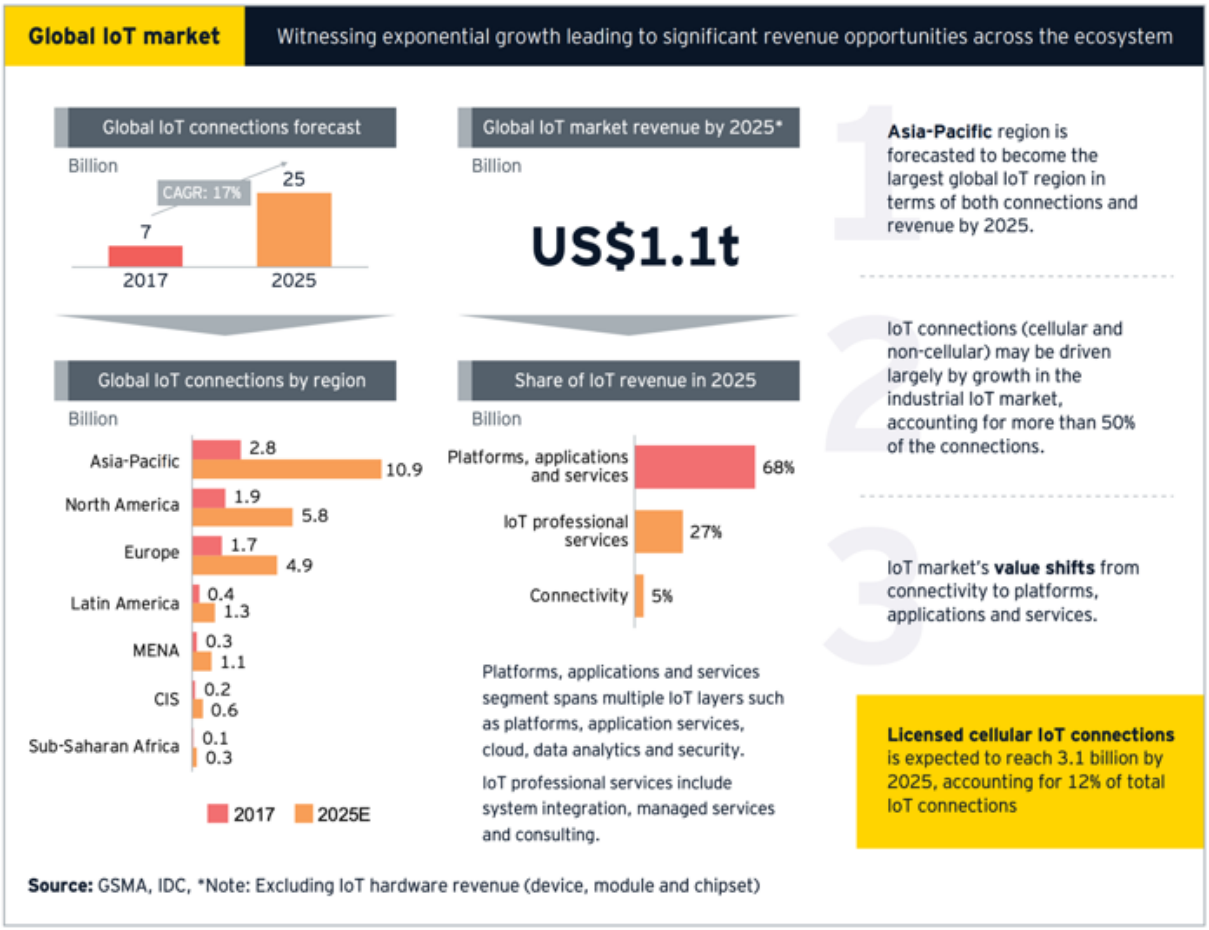


Figure 9. Market value forecast by region.[26]

A more optimistic scenario is estimated by the International Data Corporation (IDC) analysis, where worldwide technology spending on IoT is going to reach $1.2T in 2022, attaining a CAGR of 13.6% over the 2017-2022 forecast period. The consumer sector will lead IoT spending growth with a worldwide CAGR of 19%, followed closely by the insurance and healthcare provider industries. From a total spending perspective, discrete manufacturing and transportation will each exceed $150B in spending in 2022, which makes these the two largest industries for IoT spending[27].

Another important projection is that if we integrate all of our modern-day devices with internet connectivity, the IoT market is on pace to grow to over $3 trillion annually by 2026, as reflected in Figure 10. Based on that, it is forecasted that there will be more than 64 billion IoT devices by 2025, up from about 10 billion in 2018, and 9 billion in 2017[28].

[25] http://ficci.in/spdocument/23092/Future-of-IoT.pdf
[26] http://ficci.in/spdocument/23092/Future-of-IoT.pdf
[27] https://internetofbusiness.com/iot-spending-to-hit-1-2-trillion-by-2022-claims-idc/
[28] https://www.businessinsider.com/internet-of-things-report?IR=T

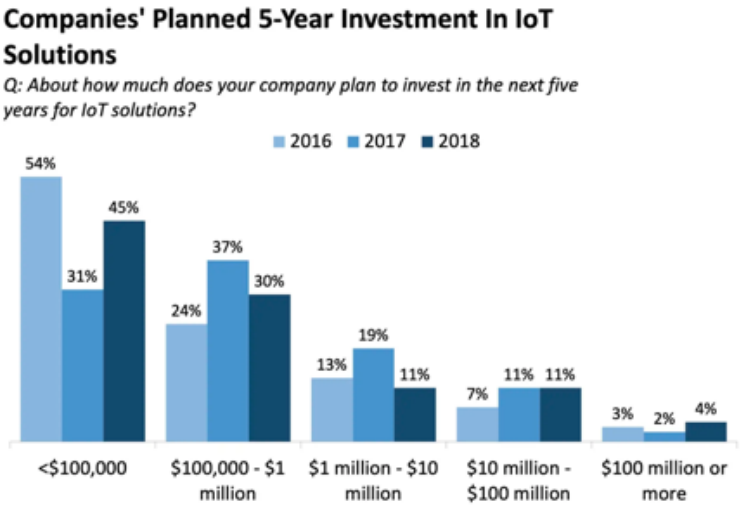


Figure 10. Planned investment on IoT solutions in the next 5 years[29]

3.2. IoT Geographical Segmentation

Geographically, the global IoT application areas and thus market, are divided into four main regions that include: North America (United States, Canada), Europe, Asia-Pacific - APAC (China, India, Japan, Australia, South Korea, & Rest of Asia Pacific) and Rest of World (Latin America, Middle East & Africa)[30]. We look into each geographical segmentation separately in order to better understand the geographical links and trends and finally also extract relevant information of the positon of Europe in the global IoT market. We use several resources with the basis being the NGIoT Scoping Paper. The figure below indicates the worldwide IoT spending.

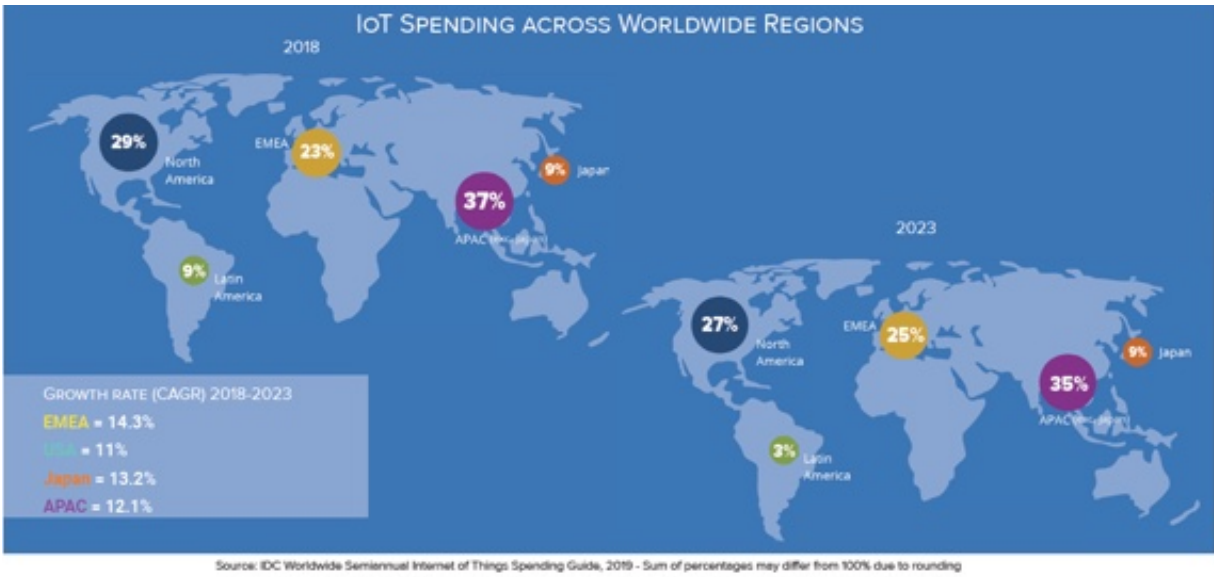


Figure 11. Worldwide IoT spending by region[31]

[29] https://www.businessinsider.com/internet-of-things-report?IR=T
[30] https://www.inkwoodresearch.com/reports/global-narrowband-iot-market-forecast-2019-2027/
[31] https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf

3.2.1. Europe

In the European Union, the applied policies, strategies and development activities have three main pillars: a **thriving IoT ecosystem**, a **human-centric approach** and a **single market for IoT**. This has been the European landscape since the AIOTI initiative was launched in 2015 with main objective of creating an industry driven IoT ecosystem[32]. Regarding the application domains and relevant technologies, Europe seems to be the leader in the Smart Cities domain, with the US following. This is an expected result of a long-term effort, since Smart Cities has been a key priority for Europe, being one of the most supported topics defined by the EU agenda. Furthermore, there is a high level of urbanisation in the EU. It is important to notice the difference in development from that of the United States, where the concept of smart urban space has been the main focus of successful start-ups[33]. An important initiative in the EU is the Large-Scale Pilots (LSPs) with a total budget of 100 Mio. EUR. The good results from this inititiave which is involving hundreds of SMEs throughout Europe, led to the funding of a new wave of Horizon 2020 – Digitizing Europe Initiative (H2020-DEI) in this specific area as specified in Figure 12. Another important initiative is the IoT-European Platforms Initiative formed in 2016 to build a functioning dynamic ecosystem in Europe and thus maximize the opportunities for platform development, interoperability and information sharing[34]. Europe's share of the global IoT market is forecast to increase as spending growth rises faster in EMEA (Europe, Middle East and Africa) than in other parts of the world[35]. This growth can be seen in Figure 13, with EU planning to invest in the programs, Horizon Europe, Digital Europe Programme, and Connecting Europe Facility. Since it is on the interest of this study to focus on the European region, a more in-depth analysis can be found in the European Context section.

Figure 12. LSP Projects[36]

[32] https://www.slideshare.net/futurewatch/future-watch-chinas-iot-ecosystem-update-87972342
[33] https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/aig-white-paper-iot-june2015-brochure.pdf
[34] https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2017/Oct2017CIIOT/CIIOT/4.Session2-1The%20general%20development%20trends%20of%20IoT-王思博V2.pdf
[35] https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf
[36] https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf

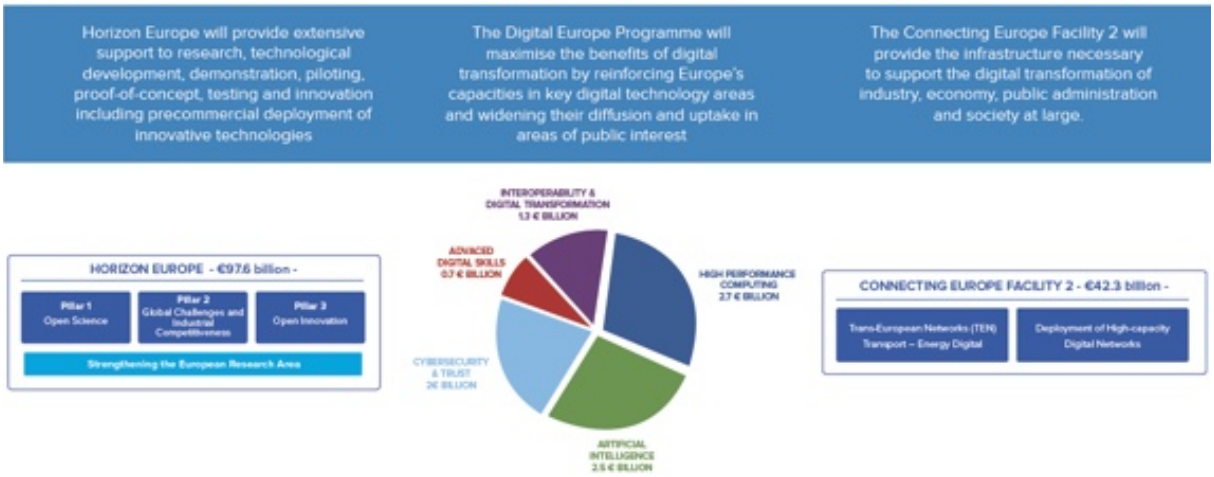


Figure 13. European Digital Investment to double in 2021-2027.[37]

3.2.2. North America

IoT centric initiatives are booming worldwide. In North America, USA, the world's leading IoT market, launched the SmartAmerica initiative in 2013 as a way to explore IoT potential across different sectors. This leads different initiatives, including US Ignite, a smart city-focused programme, that includes several projects, e.g., the Smart Giga Communities project[38], a network of communities developing a catalogue of reference applications and services to address smart city and IoT challenges. The US is mostly focusing on developing advanced manufacturing and transportation systems with IoT as part of the national IoT Strategy supported by the "Developing Innovation and Growing the Internet of Things - DIGIT" act that was introduced in 2016.[39] U.S. based companies such as Google, Cisco, and IBM are some of the leading names in IoT.

3.2.3. Asia-Pacific (APAC)

For the Asia Pacific area, there is also a high degree of activity in the connected industry domain. The APAC Internet of Things (IoT) market is expected to grow at a compounded annual growth rate of 11.3% between 2017 and 2022 to reach a market size of $95.7 billion by the end of the forecast period[40]. There was more focus on smart energy and smart cities domains during the last years. E.g. in China, similar to the US, manufacturing is the key IoT application domain, while the integration of IoT with other technologies like cloud computing, big data AI and 5G is highly encouraged and supported also by the "Made in China 2025", issued in 2015 by the State council.[41]

China is the world's largest Internet of Things (IoT) market with 64% of the 1.5 billion global cellular connections, including the rapidly growing mobile IoT licensed low-power wide-area network (LPWAN) technologies[42]. China's lead in mass deployment of innovative and transformative IoT based solutions based on mobile IoT technology, is backed by a proactive government support. There is a growing number of use cases for IoT, especially large-scale deployments across sectors in China, like Ofo's bike sharing platform or Haier's SmartHome systems[43], to cite some. On the industrial side, key players also join forces and show the benefits of the implementation of IoT (e.g. China Telecom and Huawei, Shenzhen Water and Shenzhen Gas partnership to create NB-IoT connected smart meters).

[37] https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf
[38] https://www.us-ignite.org/program/smart-gigabit-communities/
[39] https://www.slideshare.net/futurewatch/future-watch-chinas-iot-ecosystem-update-87972342
[40] https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307
[41] https://www.osborneclarke.com/wp-content/uploads/2019/04/How-will-IoT-transform-industry-in-Asia-2019.pdf
[42] https://futureiot.tech/gsma-china-is-worlds-largest-iot-market/
[43] https://www.slideshare.net/futurewatch/future-watch-chinas-iot-ecosystem-update-87972342

Also, the economy of China has shifted and now demans considerably more high-level workers for its high-tech industries. The Made in China 2025 Plan targets emerging industries such as robotics, autonomous and electric vehicle manufacturing, artificial intelligence (AI), biotech and aviation. The state provides these industries with subsidies, low-interest loans, rent-free land and tax breaks with the aim of optimising the structure of Chinese industry by emphasising quality over quantity.[44]

In terms or innovation and R&D in Asia, the scene is led by **Japan**, a forefront country on technology innovation. IoT experiments started in Japan in 2010, focusing on large-scale pilot projects on smart grid and smart community. In 2017, through the 'Artificial Intelligence Technology Strategy'[45], Japan switched the priority from the digitalisation of physical infrastructures to the extraction of intelligence from the collected data from physical infrastructures. The focus of the initiative is on three primary areas: productivity, healthcare & welfare, and mobility. Important in the strategy is the investigation of social and biological-related aspects of adopting AI, thus fostering a multidisciplinary approach.

Beyond Japan, innovation focused countries such as Hong Kong, Singapore, India and Malaysia are in the implementation phase of their IoT roadmaps. In India, the primary focus of IoT implementation lies in the manufacturing sector[46].

Singapore launched in 2014 the Smart Nation initiative[47], to lead the transformation of the country through innovative technologies leveraging the collaboration between public and private actors. In 2019, one of the core projects of the initiative was publicly released: Smart Nation Sensor Platform[48], a nation-wide platform to integrate sensors to provide services to citizens. Going beyond the Smart City area, in 2017, Singapore's Agency for Science Technology and Research launched the Industrial Internet-of-Things Innovation (I^3) programme[49], focusing on challenges to innovate industry through IoT. Priorities include: Robust data extraction in a harsh and unpredictable environment, Intelligent and secure data processing and transmission at the edge, and Effective data analysis for operational insights.

In **Malaysia**, the National IoT Strategic Roadmap[50], released in 2015, sets the ambitious goal of transforming Malaysia into the Premier Regional IoT Development Hub, focusing on priority application scenarios such as: Connected Healthcare, Traceability of assets, Home & Community Living, and People-friendly Commuting.

Emerging economies, like **India**, are working to keep pace with the rest of the world. Following the release of the "Policy on the Internet of Things" in 2016, India aims to establish 100 smart cities by 2022[51]. The policy stresses the importance of modernizing the agri-food sector through IoT in India, increasing its sustainability. The policy was recently supported by other initiatives, such as the National Digital Communications Policy (NDCP) 2018[52] aiming at innovating the digital infrastructure of the country (from networks to digital platforms and related policies) with the aim of accelerating Industry 4.0 deployment in India.

3.2.4. Rest of World

In Latin America, Mexico is aiming at leading the Industry 4.0 market, as declared in the document 'Crafting the Future: A Roadmap for Industry 4.0 In Mexico'[53] released by the Ministry of Economy in 2016. The strategy defined in the document aims at ensuring Mexico's leadership on IoT applications

[44] https://www.osborneclarke.com/wp-content/uploads/2019/04/How-will-IoT-transform-industry-in-Asia-2019.pdf
[45] https://www.nedo.go.jp/content/100865202.pdf
[46] https://www.osborneclarke.com/wp-content/uploads/2019/04/How-will-IoT-transform-industry-in-Asia-2019.pdf
[47] https://www.smartnation.sg/
[48] https://www.smartnation.sg/what-is-smart-nation/initiatives/Strategic-National-Projects/smart-nation-sensor-platform
[49] https://www.a-star.edu.sg/Research/Research-Focus/Infocomms/IIOT
[50] https://www.mestecc.gov.my/web/wp-content/uploads/2017/02/IoT-Strategic-Roadmap-1.pdf
[51] http://smartcities.gov.in
[52] dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf
[53] http://promexico.mx/documentos/mapas-de-ruta/industry-4.0-mexico.pdf

in Latin America and positioning it among the five leading countries in digital solutions and Big Data analysis in 2025.

In Africa, the leading country is South Africa, aiming to emerge as the primary IoT actor on the continent, as outlined in the document "National ICT Integrated White Paper"[54] released in 2016. The document, which has a broader scope, covers the challenges the government should take account of in relation to IoT: privacy of consumers and businesses; security for critical devices and systems; incentives to promote fair data sharing; and new regulations to data ownership control and artificial intelligence.

[54] http://www.nstf.org.za/wp-content/uploads/2017/04/National-ICT-Policy-White-Paper.pdf

4. IOT DOMAINS AND VALUE CHAIN

This section derives from the identification of the most important IoT domains from the survey elaborated during the elaboration of the Scoping Paper. The main objective is to state the importance and main applications of IoT in the different industry domains, describe these domains as well as, in general terms, the IoT value chain.

4.1. IoT in different Industries

According to Statista, 90% of senior executivess in technology, media, and telecommunications industries say IoT is critical to some or all lines of their business in 2018. 54% are very confident that their company was building sufficient digital trust controls into their IoT programs[55]. According to Bain, the security, IT/OT integration and unclear ROI are the greatest barriers to IoT adoption today. Bain & Company's conducted a survey of their enterprise clients, which reflects the broader market's high priority on securing and integrating IoT networks. Interoperability, data portability, vendor risk, and network constraints continue to escalate with clients since the latest survey completed in 2016[56].

KMPG surveyed 750 tech leaders and the key takeaway is that according to the respondents, IoT will drive the greatest business transformation in the next three years. The survey also predicts IoT will lead to the next indispensable consumer technology and has the greatest potential to drive the greatest benefits to life, society and the environment[57]. According to PwC, integrated end-to-end supply chain planning and connectivity for Industrial Internet of Things (IIoT) projects are the two areas where IoT leaders have the greatest competitive leads today. Digital innovators are also investing heavily in automating Manufacturing Execution Systems (MES) with IIoT technologies[58]. Capgemini identifies five highest potential uses cases of IoT as Environmental monitoring, smart metering, inventory intelligence, renewable plants supervision and operator productivity[59].

McKinsey states that the majority of companies who are successful in launching IoT-enabled products consider the inclusion of new connectivity options a line extension, not an entirely new product. Most successful companies launching and selling IoT products rely on their existing proven platforms as a foundation for growth[60]. Deloitte identifies that the IoT market growth will be driven primarily by Manufacturing and Automotive industries' reliance on connected unit product strategies, with Transportation & Logistics forming the largest share of industry specific IoT revenue[61]. Also, the CIO position in companies will bring more responsibility, as by 2023, the average CIO will be responsible for more than three times the endpoints they manage in 2018. New business models and the revenue streams they represent will lead to a proliferating array of new IoT networks and sensor devices supporting them[62].

As seen in Figure 14, EY predics that IoT spending among manufacturers will be largely focused on solutions that support manufacturing operations and production asset management. In transportation, more than half of IoT spending may go toward freight monitoring, followed by fleet management. IoT spending in the utilities industry may be dominated by smart grids for electricity, gas and water.[63]

[55] https://www.statista.com/statistics/945058/worldwide-iot-importance-digital-trust-industry/
[56] https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things/
[57] https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2018/06/pl-The-Changing-Landscape-of-Disruptive-Technologies-2018.pdf
[58] https://www.pwc.pt/pt/temas-actuais/pwc-apresentacao-iot.pdf
[59] https://www.capgemini.com/wp-content/uploads/2018/03/dti-research_iot_web.pdf
[60] https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/what-it-takes-to-get-an-edge-in-the-internet-of-things
[61] https://www2.deloitte.com/content/dam/Deloitte/in/Documents/manufacturing/in-mfg-harnessing-the-power-noexp.pdf
[62] https://www.centrify.com/education/what-is-zero-trust/
[63] http://ficci.in/spdocument/23092/Future-of-IoT.pdf

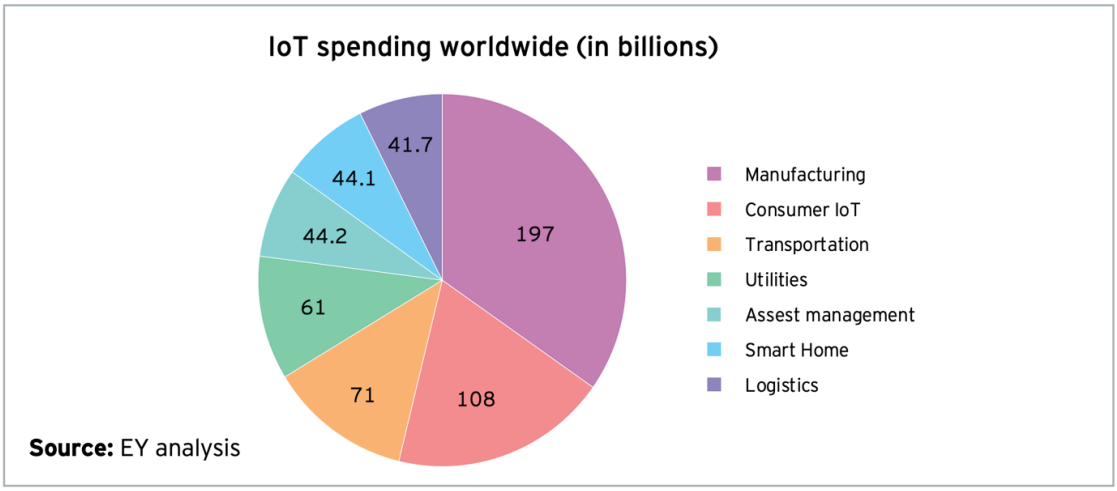


Figure 14. IoT spending worldwide

In summary, as stated by the study made by EY and FICCI[64], IoT enables real-time monitoring of the product performance which leads to better insights and faster development of new products. It is also of increasing importance the combination of IoT with powerful analytics, seen as key in automating and improving the decision-making in businesses. Also, nowadays, IoT generated data are used for detection of anomalies and control. Yet, in the future with the increased technology and analytics tools, IoT generated data might be used for predictive analysis and optimizations, leading to new opportunities and innovative business models. This leads to questions about where these new tools can be applied, how is data security and privacy handled, and therefore what adequate policies and frameworks, in general terms and for each of the main domains.

4.2. IoT industry domains

Because different studies propose different segmentation in term of domains, this report will use the domains selected for the survey done for the Scoping Paper. More details about the specific impact, transformation potential and consolidated opportunities related to the exploitation of IoT technologies can be found in the analysis in section 0. The pertinent domains to this study are:

- **Energy Management:** everything related to power generation and distribution.
- **Manufacturing:** from efficiency gains to optimization of supply chains.
- **Transportation:** covers the logistics issues from industrial to commercial transportation.
- **Smart Cities & Communities:** solutions for better governance and collective life quality.
- **Smart living:** home automation through connected smart appliances.
- **Healthcare:** from wearables to specific healthcare applications.
- **Smart Food & Farming:** from food production to processing and distribution.
- **Retail:** everything related to the last linkage of the traditional value chain, the end-customer.
- **The Media:** Advertising and customer-targeting.
- **Insurance:** any kind of risk assessment and protection.
- **Safety and Defence:** from emergency response to better monitoring.

[64] http://ficci.in/spdocument/23092/Future-of-IoT.pdf

4.3. IoT Value Chain

In order to understand how value is created in an IoT context, it is useful to have a basic understanding of the IoT value chain. Because of its nature, which allows the use and re-use of data, the value chain becomes non-linear and it is difficult to represent it in a single dimension. The CREATE IoT project divides the value chain in horizontal and vertical, where the former represents the flow of data and the latter the specifics of segment being analysed[65]. Because of this cross-cutting nature of IoT, it is difficult to represent the value independently on the vertical that is being analysed. For instance, the application of this technology in a vertical like the healthcare industry, will not be the same as the one for the automotive industry.

However, Figure 15 represents a general approach that can be incorporated in different verticals. Each of these linkages represent a value capturing opportunity. Figure 16 shows an approximate share of value capture for each of the linkages, however, this percentage varies from one industry to the other. As a matter of example, Figure 17 shows the value chain for the automotive and the healthcare industry, with the biggest players nowadays. It is also important to notice that in some industries like healthcare, companies are using the joint venture model in order facilitate the development of new products and services.

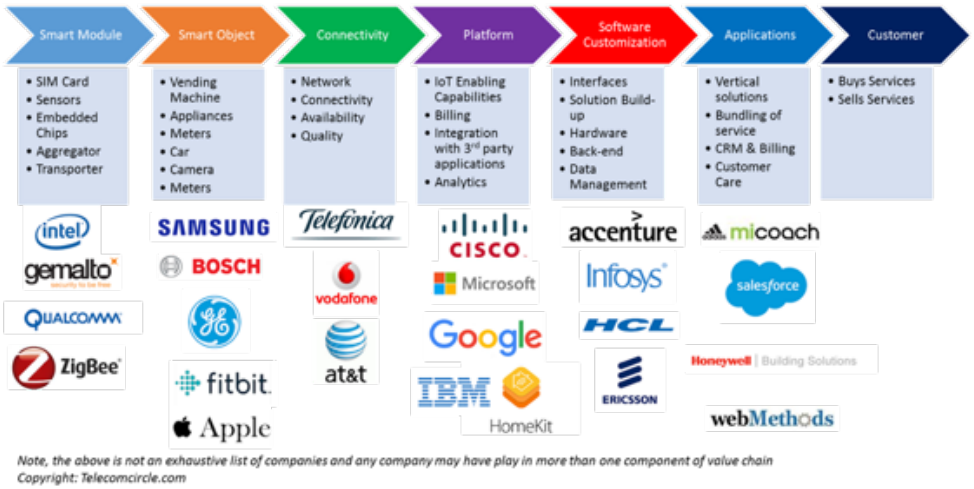


Figure 15. IoT Value Chain[66]

[65] For a detailed description of the IoT value chain see Create IoT project, *IoT Data Value Chain Model*, September 2017, available at: https://european-iot-pilots.eu/wp-content/uploads/2017/10/D05_03_WP05_H2020_CREATE-IoT_Final.pdf.
[66] https://www.telecomcircle.com/2016/05/internet-of-things-business-models/

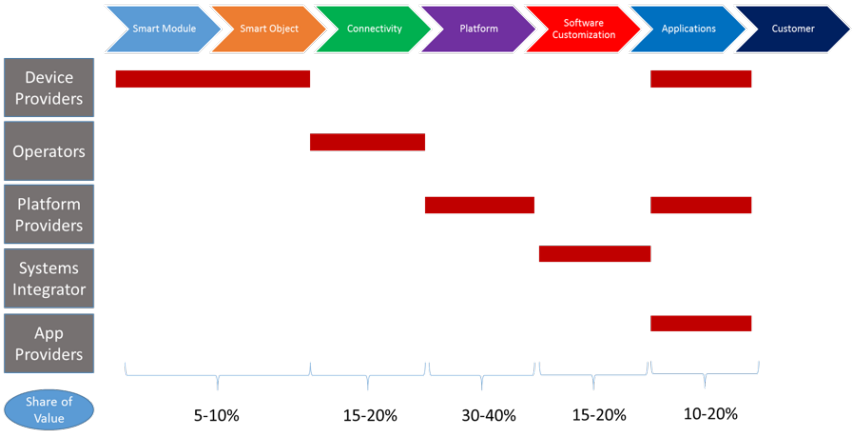


Figure 16. IoT value chain share of value[67]

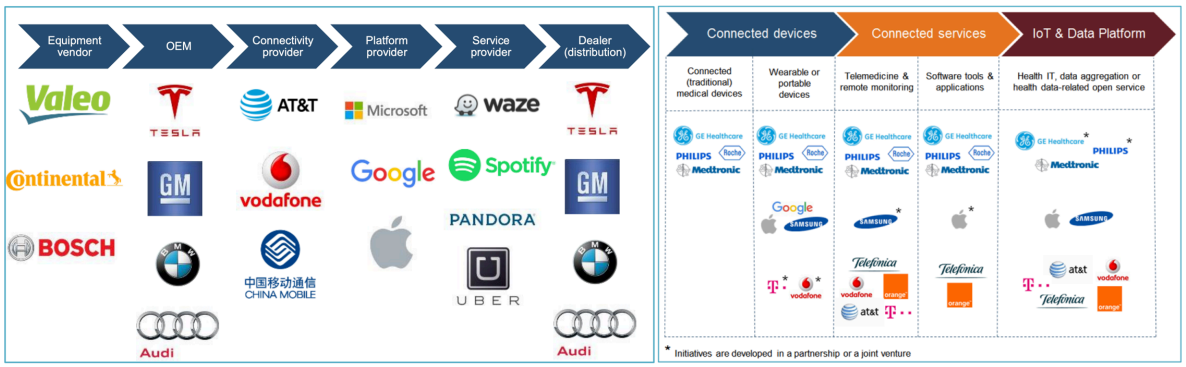


Figure 17. Value chain examples[68]

[67] https://www.telecomcircle.com/2016/05/internet-of-things-business-models/
[68] https://european-iot-pilots.eu/wp-content/uploads/2017/10/D05_03_WP05_H2020_CREATE-IoT_Final.pdf

5. IOT TECHNOLOGY DRIVERS

5.1. IoT relation to other transformative technologies as drivers for R&D

Current IoT market trends could be expressed as being extremely dynamic, but there are a few dozen trends that can be observed, including edge-to-cloud integration, TSN connectivity, and IoT&blockchain trials (for example cloud vendors now increasingly make their own cloud-ready hardware to improve the interoperability and performance between IoT devices and the data that gets stored and analyzed in public or private clouds). Leading IoT cloud providers Microsoft, Amazon, and Google all recently announced their own hardware[69].

Recent roadmaps and strategic agendas related to Internet of Things, evidence the role and relation with other technologies and how IoT advancement is strictly connected to these. In particular, the last few years witnessed the appearance of a number of innovative (and in some cases disruptive) technologies. Some of the key related technologies are:

- **Edge and Cloud computing:**

Surging as complementary paradigms of data processing and storage, these drivers of IoT balance the location of computational power and storage at the edge of the network and through the internet.

- Characterization: the industrial internet consortium defines edge computing as a "decentralized computing infrastructure in which computing resources and application services can be distributed along the communication path from the data source to the cloud"[70], where the cloud represents the data centres and infrastructure at the end of the network. In Figure 18[71] IDC mapped 4 layers of edge computing: packaged endpoints, light edge, heavy edge and distributed core[72].

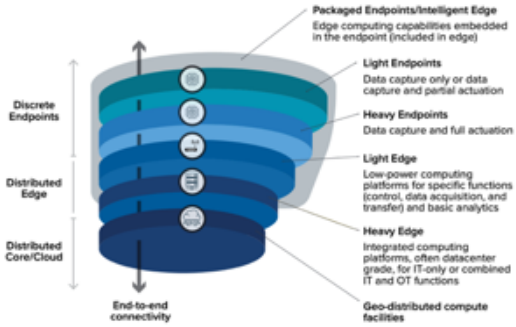


Figure 18. Edge Computing Layers

- Relation to IoT: the increasing IoT requirements of real time data collection, process, analysis and actuation drive the development of optimal edge computing solutions. Key drivers for edge adoption within IoT are the increasing data volume, the need of minimal latency, communication in remote areas, and data privacy and security[73]. Gartner estimates that driven by IoT, data processing outside of the data centres will pass from 10% to over 75%[74].
- Worldwide initiatives and players:
  - Cloud: Amazon AWS, Google Cloud, Microsoft Azure and IBM Cloud are the biggest cloud providers worldwide[75], followed by Alibaba Cloud which plays the biggest role in China, whereas in Europe the landscape is more fragmented.

[69] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/
[70] https://www.iiconsortium.org/pdf/Introduction_to_Edge_Computing_in_IIoT_2018-06-18-updated.pdf
[71] https://blog-idcuk.com/everything-is-edge-and-edge-is-everywhere/
[72] https://www.rtinsights.com/wp-content/uploads/2020/05/The-Edge-Cloud-Enabling-an-Intelligent-Digital-World.pdf
[73] https://www.iiconsortium.org/pdf/Introduction_to_Edge_Computing_in_IIoT_2018-06-18-updated.pdf
[74] https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/
[75] https://www.gartner.com/en/newsroom/press-releases/2019-07-29-gartner-says-worldwide-iaas-public-cloud-services-market-grew-31point3-percent-in-2018

- Edge: as a fragmented and relatively young industry, the biggest players come from cloud providers and other knowledgeable companies. With Microsoft notably holding over 300 patents[76], Amazon (Greengrass, FreeRTOS, Lambda@Edge), DELL CME, HPE, IBM Edge Computing and Cisco Edge and many other smaller companies play an important role. Edgeir provides an extensive company list[77] with some big, medium and small players worldwide.

- **5G/6G:**

This technology driver refers to the new generation of mobile communication that supports a massive number of devices with a diverse range of speed, bandwidth and quality of service.

- Characterization: the fifth generation of mobile cellular technologies encompasses reliability, latency, scalability, security and ubiquitous mobility. As seen in Figure 19 and stated by the 5G Observatory, 5G's objective is to provide the right throughput to the right user[78], dividing the service in 3 big scenarios according to the application needs[79].

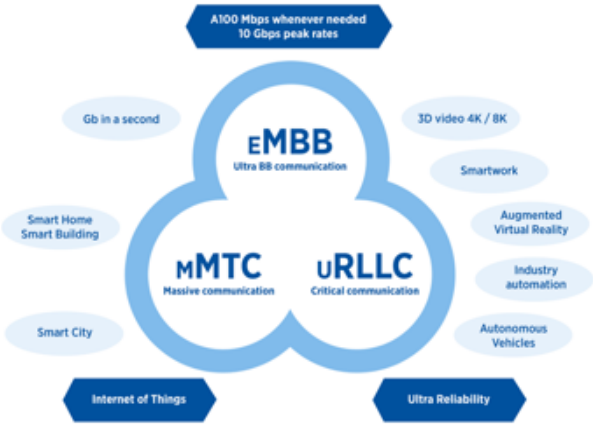


Figure 19. 5G Usage Scenarios

- Relation to IoT: cheap, reliable and scalable internet connectivity is a key requirement for several IoT scenarios. With its augmented spectrum, 5G aims to tackle requirements posed by IoT large deployments beyond what today is possible with LPWAN, achieving massive and critical communications with a complete vision deployed by 2021[80].
- Worldwide initiatives and players: besides the 5G providers, McKinsey identified 3 main players poised to win: component suppliers, industrial automation companies and manufacturers[81]. In terms of providers, the clear global players are Ericsson, Nokia and Huawei. As for the component suppliers, the providers vary within the EMBB, URLLC and MMTC scenarios, with Qualcomm, Skyworks, Intel, Broadcom and Xilinx[82] as some of the top firms.

[76] https://www.zdnet.com/article/10-edge-computing-vendors-to-watch/
[77] https://www.edgeir.com/edge-computing-companies
[78] https://5gobservatory.eu/about/what-is-5g/
[79] https://www.gsma.com/iot/wp-content/uploads/2019/11/201911-GSMA-IoT-Report-IoT-in-the-5G-Era.pdf
[80] https://www.traficom.fi/sites/default/files/media/file/Putkonen%20Jyri_5GMomentum_5GIIoT_JPutkonen_20191029.pdf
[81] https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/the%205g%20era%20new%20horizons%20for%20advanced%20electronics%20and%20industrial%20companies/the-5g-era-new-horizons-for-advanced-electronics-and-industrial-companies.ashx
[82] https://www.cnbc.com/2019/02/06/cramer-here-are-the-5-biggest-beneficiaries-of-the-5g-rollout.html

- **Artificial Intelligence:** Blended with IoT, AI offers augmented intelligence in the data analysis process. The availability of massive data sets to train, test and apply AI (Big Data) [83] combined with increasing computing capability (HPC[84]) enabled its wide adoption in several real-life scenarios. This combination is expected to kick off the next wave of performance improvements, especially in the industrial sector[85], by enabling extraction of unexpected 'intelligence' from sensed data, the automatic actuation based on 'intelligent' models (e.g. self-driving cars), the higher automation in the management of a plethora of devices and their generated data. Also, as Artificial Intelligence becomes a reality across several application[86], its combination with IoT is moving towards the edge[87], enabling usage of algorithms closer to the devices.

- **Augmented Reality and Tactile Internet**: IoT can act as a broker between the assets of the physical environment and the digital infrastructures, while AR serves and supports the digital interaction in real time with the physical environment. The combination of these two technologies has, and still is leading to new possibilities, experiences and applications in all the domains where extreme or difficult conditions from real life (low visibility, accessibility, remote locations, high temperature, etc.) must be faced and overcome. Thus, adding the AI dimension to IoT expands enormously its possibilities in all verticals. It is widely considered that IoT platforms will move rapidly and with big steps to the next level with the emerging 'Tactile Internet and the intelligence at the edge, creating interactive, conversational IoT platforms with new user interfaces to engage with things and humans'[88], adding the human-centred perspective and sensing/actuating capabilities in the human-objects-systems interaction[89]. Of course, the key enablers for this to happen are powerful devices and high-performance networks.

- **Digital Twin:** more than a technology, the digital twin is a concept that relies on the combination of different technologies (IoT, artificial intelligence, machine learning and software analytics) to realise the digital replica of a living or non-living physical entity. The aim of this approach is the ability to monitor, control and simulate in the most realistic way a physical system. The approach is largely advocated in the manufacturing and healthcare sectors and brings new challenges to the understanding of the relation between the digital world (as sensed by IoT devices) and the physical world (humans included). Such relation in the digital twin concept often explores the 'human' side of the interaction between humans and machines, aiming to understand how humans perceive and interact with the technologies.

[83] https://novarica.com/big-data-iot-and-ai-incremental-phases-grow-value-says-novarica/
[84] https://insidehpc.com/white-paper/ai-hpc-happening-now/
[85] https://www.mckinsey.com/~/media/McKinsey/Industries/Semiconductors/Our%20Insights/Smartening%20up%20with%20artificial%20intelligence/Smartening-up-with-artificial-intelligence.ashx

[86] https://novarica.com/big-data-iot-and-ai-incremental-phases-grow-value-says-novarica/
[87] https://www.i-scoop.eu/internet-of-things-guide/building-management-systems-iot/
[88] https://aioti.eu/wp-content/uploads/2018/09/AIOTI_IoT-Research_Innovation_Priorities_2018_for_publishing.pdf
[89] Petar Popovski (2018), "The Supernatural Touch of Tactile Internet, Big Data, AI, and Blockchain", https://medium.com/@petarpopovski_51271/the-supernatural-touch-of-tactile-internet-big-data-ai-and-blockchain-e05f93a198d6

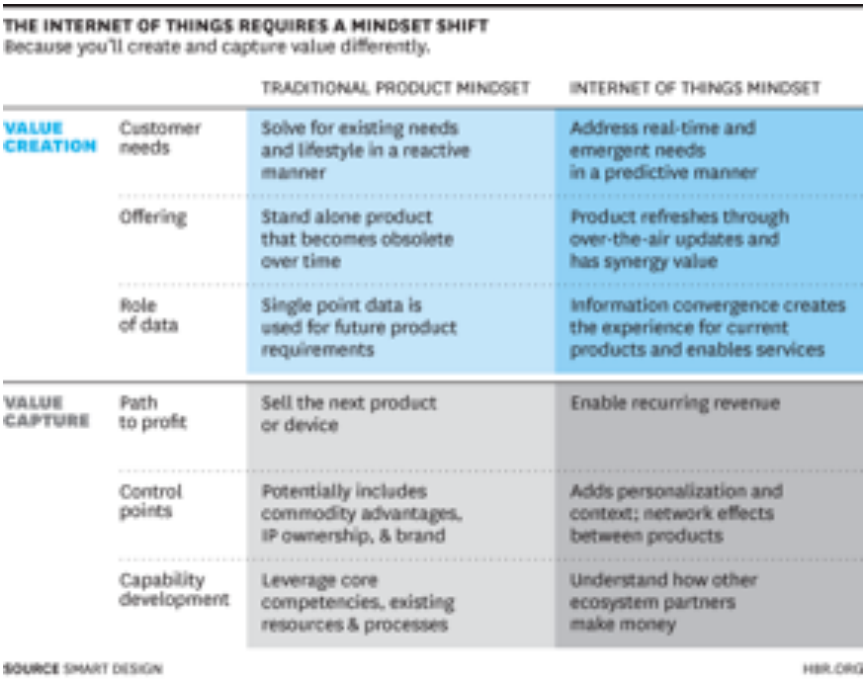
- **Distributed Ledgers:** most of the platforms dominating today's IoT market relies on centralised data management. The advent of distributed ledgers, following the hype of bitcoin derived technologies, advocates for novel approaches for data management. These approaches enable for a decentralised governance, where all the actors in the ecosystem play a role in the validation and acceptance of the data entering the ecosystem, and data owners can have direct control over who in the network can access their data. In the context of the Internet of Things, both the ability to ensure truthfulness of the data and authorising data access in a distributed way are interesting concepts. In some sectors, these technologies are becoming enablers for new scenarios around trusted data (e.g. food provenance). Despite some promising results in some IoT related scenarios, it is also true that distributed ledgers showed limited applicability in other scenarios, where for example real-time requirement is strict.

6. IOT BUSINESS MODELS

6.1. Introduction to IoT Innovative Business Models

Since the 1990s, new digital business models have disrupted the global economy. However, these new patterns of creating value have remained mostly on the digital world, providing little value to the dominant business models of the physical world. However, IoT now makes possible hybrid solutions that merge physical products and digital services[90], creating a new array of totally new business model patterns. Some of these are totally new business models, but some others are not totally new models but are instead traditional models enhanced by the new capabilities of technology and the shift in the mindset driven by these capabilities seen in Figure 20.

For example, IoT enables 7/24 hours connectivity that allows an uninterrupted revenue stream from business activities. This in turns brings a closer relationship with customers (personalization/tailoring of offerings) since IoT devices continuously gather data. This helps businesses to better understand customer needs and therefore, allows the surge of new innovative IoT related business models, which aim to get the most out of the opportunities created, e.g. by an increased revenue, increased (IoT) market share and an increased profit.[91]



THE INTERNET OF THINGS REQUIRES A MINDSET SHIFT
Because you'll create and capture value differently.

		TRADITIONAL PRODUCT MINDSET	INTERNET OF THINGS MINDSET
VALUE CREATION	Customer needs	Solve for existing needs and lifestyle in a reactive manner	Address real-time and emergent needs in a predictive manner
	Offering	Stand alone product that becomes obsolete over time	Product refreshes through over-the-air updates and has synergy value
	Role of data	Single point data is used for future product requirements	Information convergence creates the experience for current products and enables services
VALUE CAPTURE	Path to profit	Sell the next product or device	Enable recurring revenue
	Control points	Potentially includes commodity advantages, IP ownership, & brand	Adds personalization and context; network effects between products
	Capability development	Leverage core competencies, existing resources & processes	Understand how other ecosystem partners make money

SOURCE SMART DESIGN HBR.ORG

Figure 20. IoT mindset shift[92]

6.2. Key Innovative Business Models Stakeholders

There are various stakeholders involved in each business model and each vertical. For this reason, each model is very specific and thus summarizing all the key stakeholders would be lengthy and inefficient. Therefore, this section provides a picture of the basic IoT ecosystem mapping the IoT landscape –

[90] https://www.iot-lab.ch/wp-content/uploads/2019/01/7_Fleisch_et_al_2014_Business-Models-and-the-IoT.pdf
[91] https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf
[92] https://hbr.org/2014/07/how-the-internet-of-things-changes-business-models

stakeholders in (e.g. standardisation provider, service providers, marketplace providers etc.) as well as the incentives, tools and money flow between the stakeholders.

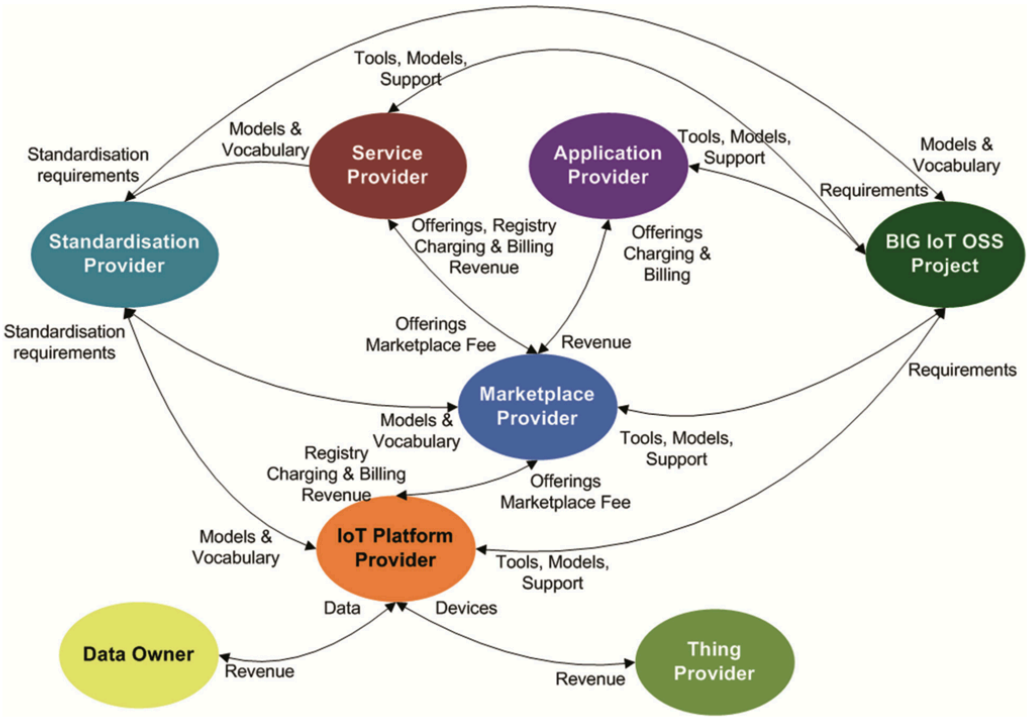


Figure 21. Value network model for Interoperable IoT systems[93]

6.3. Innovative IoT-related Business Models

Taking the definition of a business model as the rationale of how an organization creates, delivers, and captures value[94], the following business models were identified as being influenced by IoT. It is important to clarify that there is no consensus on a single list of business models surrounding the IoT technology, but rather different flavours of the same ideas are usually combined and used in multiple ways by the different companies. For this reason, these 7 models were chosen as a way of trying to englobe the most common models, even if some overlaps can be seen between them depending on the implementation chosen by the different stakeholders.

6.3.1. Subscription Model

Customer pays a fee in return for continuous value or asset. The value or asset is provided for a specific amount of time in return for a fee. (e.g. similar to leasing schemes)[95]. This model is easily understandable by customers and it can be easily adjusted. Nowadays, there is a considerable opportunity in offering "IoT as a Service" in the form of a subscription model. On one hand, it is quite attractive for vendors, as they have a predictable and recurring revenue stream, as the customer pays fees and is obliged to pay them for a certain contractual period. For managers, understanding the strategic importance of launching a subscription model is crucial for taking a decision if the solution is suitable to be sold using this business model, whether customers´expectations are aligned with this way of selling to them, and on how to execute it[96].

[93] Business Models for Interoperable IoT Ecosystems, Schladofsky et al., direct link to be added
[94] https://danielelizalde.com/monetize-your-iot-product/
[95] http://www.internet-of-things-research.eu/pdf/D02_01_WP02_H2020_UNIFY-IoT_Final.pdf
[96] https://www.iotforall.com/iot-subscription-strategy/

The subscription business model is useful for several IoT applications, listed below[97]:

Compliance monitoring: it is estimated that American manufacturers spend $192 B on compliance (e.g. economic, environmental, and safety regulations). IoT can remarkably reduce these costs. As an example, we can take the oil and gas extractions and processing sites, which should meet very rigourous compliance standards. Nowadays, IoT devices can remotely monitor the key compliance metrics (e.g. oil leaks, gas emissions). This reduces the costs for physical inspections and it is also more reliable. What is more, the IoT device provides constant monitoring, not only once in a pre-defined time. Thus, problems can be identified earlier and potential penalties can be considerably reduced, as often penalties are dependent on how many leaks are there.

Preventative maintenance: very important contribution to the protection of valuable in-field assets. In some industries, even small technological problems can lead to considerable decreases in efficiency and significant losses. Thus, there is a clear incentive to install an IoT device (comparably inexpensive) that remotely monitors equipment, tracks maintenance schedules and thus prevents malfunctions. Similar to the compliance monitoring, the data transmitted are continuous.

Remote diagnostics: IoT devices are also suitable to collect detailed and timely diagnostic data in a wide variety of different fields. An example could be indoor growers and nursery owners that implement IoT devices to help monitor and manage their plants. The connected IoT device continuously monitors environmental conditions such as temperature, humidity, sunlight, and soil condition. The collected data are compiled and organised to help growers analyse long-term environmental trends. The IoT devices can also be designed to respond to the evaluated data (e.g. by low moisture trigger the water system).

Asset tracking: this IoT application has the potential to dramatically increase supply-chain visibility for relatively little cost. A simple device (3G-connected microcontroller) can identify, track, and monitor an asset in real time, from anywhere on Earth. This helps companies prevent against loss and theft, increase fleet efficiencies, and improve demand forecasting. The generated data can also be shared with other stakeholders involved in the supply chain, thus increasing visibility and effcicincy. According to the DHL and Cisco estimated, IoT have the potential to have a positive impact of $1.9 T on the logistics and supply chain industry.

Automatic fulfilment: according to the up-to-the-minute inventory and consumption data, automatic fulfilment and service level agreements are made. An example is the Amazon Dash button – this small consumer IoT device is configured to reorder specific items when pressed. This provides continuous value by driving sales and by providing valuable data on customer consumption habits. Nowadays, the importance of truly automatic models increases.

6.3.2. Outcome-Based Model

Customers to pay for the outcome (or benefit) the product provides, as opposed to the product itself. This model can be paralleled with the lease services replacing the selling of a product by the selling of the outome of said product. Even if this model can be easily implemented in some industries without the need of IoT, it is now enabled by it in industries where it was unthought of. Brother, for example, the computer accessories manufacturer, offers leases for laser printers, without any base leasing rate – only the pages that are actually printed are invoiced[98]. Another application that is being implemented in some rural areas is the selling of prepaid electricity. With the ability to automate the amount of electricity being sourced to each customer individually, this model of pay-per-watt is being used in places where building the traditional infrastructure was not viable[99].

[97] https://www.itproportal.com/features/the-top-5-most-successful-iot-business-models/
[98] https://www.iot-lab.ch/wp-content/uploads/2019/01/7_Fleisch_et_al_2014_Business-Models-and-the-IoT.pdf
[99] https://www.devex.com/news/sustainable-energy-for-all-reducing-energy-poverty-in-rural-haiti-86411

6.3.3. Asset Sharing Model

Customers often do not utilize the equipment they buy to its maximum capacity, especially those with a high fixed cost, ranging from cars to expensive machinery. Because of this, sharing is more interesting in order to monetize the unused extra capacity. The goal of this business model is to maximize the utilization of the IoT product across multiple customers: each customer pays a reduced price and you are able to get faster market penetration, compared to when a single customer has to pay for your complete product. Several stakeholders can monetize from this business model, from the owners of the asset, to the platform that connects the user with the owner. Examples of this can be car-sharing or bike-sharing companies, virtual power plants, shared drones, etc. "Knowing the geographic location and availability of a device allows you to share the device with interested parties. The usage is billed according to the duration or quantity and the revenues are distributed to the respective parties via IoT Business Suite billing module according the agreements"[100].

6.3.4. The Razor-Blade Model

It can be described as designing an IoT product to sell other products. A more detailed example can be to sell the IoT product at cost or even at a loss since the goal is to get the product in the customer's hands, so you can start selling your other products. This business model can be very lucrative for products that have consumables needing constant replacement. The goal of this IoT business model is to turn a "normal" product into an IoT product to automatically reorder its consumable before it runs out. It provides "contextual shopping", meaning the ability to reorder a product right when the customer needs it. An example can be the Amazon Dash Buttons – the connected buttons are pre-configured to order a specific product. When the button is pressed, it reorders the particular item from Amazon, and it is directly delivered to the given address. This reduces the barriers to re-order and product of need. In that case, the Amazon Dash Button is not the revenue maker, but a tool to sell other products in the calatog of Amazon. In general, this model is very suitable for products that need refills (e.g. automatic orders of ink when low cartridge by "smart printers").

6.3.5. Monetize Your IoT Data Model

This is one of the most important ways of monetization of the IoT phenomena. It is the most promising new IoT-related business model offering an enormous opportunity. IoT-enabled products collect a huge amount of data and more important than the data themselves are the insights that can be derived from the data collected. The real value of these insights can be when they are provided to third party companies such as advertisers that use the data to promote their products and services. In IoT in particular, the product can be built to provide value to the end user and also to collect defined valuable data that can be sold to an interested third party. With this approach, the IoT device can be offered at no cost to eliminate the buying friction for the end user. The goal is to deploy as many devices as possible to collect data. The objective is to build a network effect. The more devices a business entity has out there, the more attractive its data proposition will become to third parties.

There are many examples of products leveraging this IoT business model, such as energy efficiency devices installed in buildings to monitor their energy consumption. The building manager surely benefits from this data, but utilities or other aggregators are willing to pay an important sum to receive aggregated data from thousands of buildings. Another example can be devices monitoring driver's habits for car insurance companies, which gives them the possibility to better understand individual risks and adjust the premia, leading to better efficiency and portfolio optimalization. The producers of these devices can sell these data to insurance companies and make profit[101]. Many companies already

[100] https://digitalrepublic.ch/wp-content/uploads/2018/04/Digital-Republic-IoT-Business-Models-EN-HQ.pdf
[101] https://www.iotforall.com/iot-business-model-monetize-product/

stepped-in in this market and specialize on the data monetization model. The accumulated and anonymized information is offered as packaged or raw form or through advertising[102].

However, there are some challenges to overcome in order to fully use the potential of the IoT-collected data monetization. A significant challenge is the data quality – especially accuracy, completeness, integrity, timeliness and building trust at customers of the data provided. Another obstacle is the determination of types of information required – companies looking for IoT data might need them in different forms and data additional data points have to be recorded. This requires a huge amount of flexibility. Data and service around them require a new way of seeling and activities around it – research, design, promotion, support. Data security and protection against unintended/unlicenses uses is also a great obstacle to overcome – a possibility is through special contracts. Companies like Amazon, Google, Facebook and Mictosoft are constantly learning to provide solutions and have the possibility to build different models and even make pilot studies[103] around this idea.

There is an interesting Data Economy Framework developed by IBM with the most common stakeholders entering the process and the value they bring in the system, Figure 22. Data collected, analysed and sold can create value by both cost reduction or increase of revenue by enhancing existing products or creating new ones. Figure 23 provides an overview of the main data types generated that can be further resold[104].

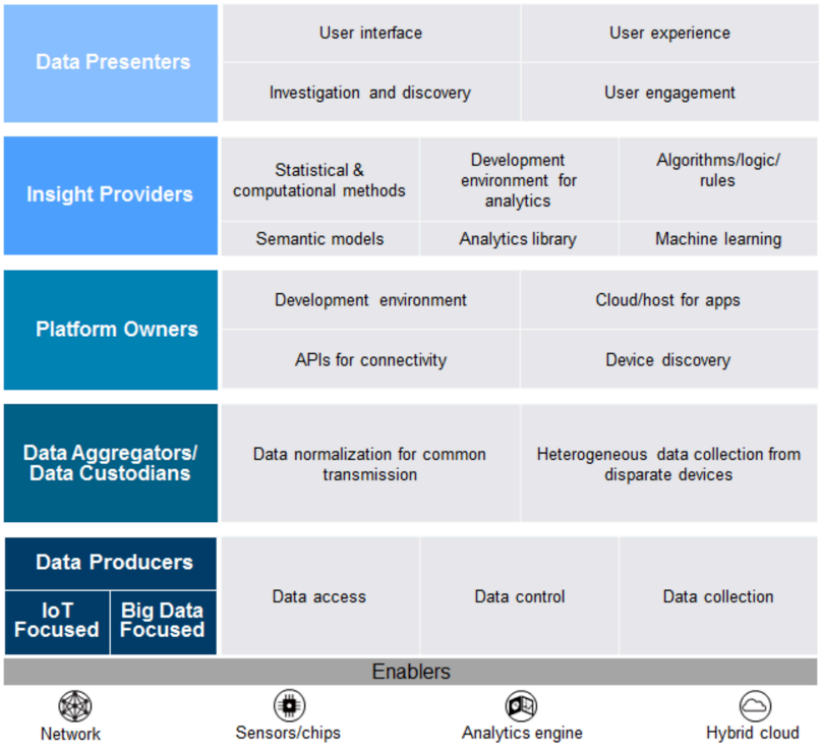
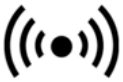


Figure 22. IBM´s Data Economy Framework

[102] https://thinkmobiles.com/blog/iot-monetization-how-to-make-money-on-your-product/
[103] https://dzone.com/articles/how-data-monetization-is-creating-a-new-data-econo
[104] https://www.ibm.com/downloads/cas/4JROLDQ7

Common IoT data types	Description	Examples
Location 	Where a particular thing is positioned geospatially. Typically identifies a location based upon GPS, wi-fi, beacon, or simply asking a user for their location.	Uber knows the location of its users based upon their pick-up and drop-off locations. With the users' permission, Uber may sell this data to other businesses. Businesses use this data to provide promotions that encourage consumers to spend money with their company. Uber launched a service that lets its customers connect their Uber account to their Starwood Preferred Guest Account. When a Starwood customer is traveling and they don't choose Starwood, they can receive promotions.[2]
Environment 	Based on the measurement of environmental variables (i.e. the state of the environment)	A wind farm company is looking to expand into new areas. By utilizing wind sensors, the company is able to identify the locations that have the greatest energy generation potential and maximize their return on investment. After identifying their future locations, the wind farm company can continue to monetize its wind sensors by selling the data to weather companies looking to supplement their own sensors.
Machine 	Data that is automatically created from a computer process, piece of equipment, application, or other machine without the intervention of a human	IoT devices that interface with a vehicle's computer can sense driving speed, braking force, acceleration, engine problems, and a variety of other diagnostic information. This data can be used by insurance companies and can also be packaged and resold to a variety of other industries. For example, engine and diagnostic information are valuable to automotive companies that want to prevent systemic mechanical issues on vehicles or automotive repair shops looking to improve their marketing campaigns.
Living 	Data collected from sensors that monitor vitals (e.g. blood pressure, heart rate, temperature)	Pharmaceutical companies looking to improve sales can purchase anonymized health data that is generated by IoT sensors in order to find new customers and more effectively target their product marketing.
Event 	Point at which an affair or occurrence transpired	As sports fans move through future stadiums, they will be greeted with incentives from nearby stores that are customized to each specific fan's interests. With offers that appeal to each individual fan, sports franchises will have the opportunity to sell more products and increase revenues.
Attribute 	Characteristic of an object that can be categorized and/or counted	A TV manufacturer wants to ensure that display units are properly calibrated to reduce after-sale support and warranty repair. By measuring color quality and luminosity of display units while still on the production line, the manufacturer can ensure its products are within benchmarks.
Motion 	Movement or position of an object or human being	Companies measure forms of movement in 3D space and compare it against the ideal model. For example, an instrumented cyclist may be compared against a professional cyclist and an accompanying real-time virtual coach could provide feedback to improve form and speed.
Orientation 	Relative position of an object	The orientation of a smartphone determines specific actions. For example, if a smart phone is face down, it can be switched to do-not-disturb mode.

[2]http://www.forbes.com/sites/ronhirson/2015/03/23/uber-the-big-data-company/

Figure 23. Main types of data generated by IoT

6.3.6. Monetising consumer connectivity with M2M data buckets:

"One of the challenges in cellular networked products is the cost of connectivity, which has to be included in the product for the markets over the lifecycle of the product. As a result, although the product is connected and smart, it increases the sales price and makes it more difficult to compete. Integrating the IoT Business Suite with the M2M Connectivity Management Platform enables the offering of Data Buckets and Connectivity on Demand for consumers. This helps manufacturers to offer a complete product to their consumers with a SIM-based connectivity solution including branded and user-friendly web cockpits, e.g. Internet in the car products for WiFi and infotainment applications.[105]"

6.3.7. Pay-Per-Usage Models

IoT-enabled products can easily monitor via sensors on the hardware device the amount of services used by a customer and their environment like never before. This gives to option to charge the customer according to the active time he uses a service or a product. The main revenue does not come from the device itself, but from the data generated by the IoT device to track the usage parameters. An example could be the Metromile insurance company in San Francisco. They offer car insurance with premiums calculated according to the usage of the car which translates to the risk calculation and per-mile price for the insurance[106].

"The IoT brings the possibility of measuring the usage of a device. In a pay-per-use business model, the use of a product or service is measured, and customers are charged when they use the service. This can lower the acquisition cost and enable sustainable recurring revenues. The usage data can be determined via the IoT application, evaluated with the Rating & Pricing Engine of IoT Business Suite and settled directly with the consumer"[107].

This model is very suitable for elastic workload demands and for applications that need access to an unlimited resource pool. Revenue and expenditures are very volatile as they are based on consumption[108]. This business model is very similar to the outcome-based model, however, the pay-per-usage is more oriented to services, whereas the outcome-based relates more to products and generally requires a more tangible outcome than timing the utilization of an asset.

6.3.8. Offer-a-Service Model

IoT products allow to develop new ways of differentiating in the traditional service industry. The idea is to enhance actual existing services that cannot be automated, yet. An example is to use an IoT product to monitor machinery, predict maintenance, and then sell a maintenance contract. A good example of this is the improvement that some elevator companies are doing, like Kone's new Kone Care 24/7 monitoring and maintenance[109]. Other examples include the installation of IoT devices in a smart building to measure energy consumption. Then sell an energy audit and energy optimization services. Or the implementation of IoT devices in a manufacturing floor to measure efficiency and throughput in order to sell consulting services to optimize your customer's process.

[105] https://digitalrepublic.ch/wp-content/uploads/2018/04/Digital-Republic-IoT-Business-Models-EN-HQ.pdf
[106] https://danielelizalde.com/monetize-your-iot-product/
[107] https://digitalrepublic.ch/wp-content/uploads/2018/04/Digital-Republic-IoT-Business-Models-EN-HQ.pdf
[108] https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Subscription-and-pay-per-use-IoT-revenue-models
[109] https://www.kone.us/Images/kone-care_tcm25-18798.pdf

7. EUROPEAN CONTEXT

A PESTLE analysis was conducted in order to understand Europe's position regarding the IoT. This analysis aims to understand the main pain points a company would face on the European macro-environmental landscape. Afterwards, an overall assessment of Europe's position in terms of research, innovation and deployment summarizes where Europe stands on a global competitive landscape. This works as starting point to compare the priorities based on external studies and the ones from the survey result from the scoping paper.

7.1. PESTLE analysis

Political	• European Comission solidity • Brexit could potentially hit the Digital Single Market Initiative • Data privacy and protection is a priority amongst the European citizens
Economical	• Europe has the highest growth potential for IoT. • Multiplier effect of Big Data. • Likely trade surplus, M2M connections proxy • Shift in labour skills • High cost of large-scale implementation among other barriers
Societal	• Lack of transparency and scepticism • Concerns about personal security • Shortfall of digital knowledge and skills • Equal access for consumers and SMEs
Technological	• Lack of low-cost connecting services – smartphone/internet penetration • Costs of Big Data tools and AI development • Declining high-tech competitiveness despite high R&D investments • Edge still not mature – no reference frame from ECCE, fragmented market
Legal	• Competition Law on big data management • Personal Data Protection - GDPR • Standardisation • International flow of data • Missing regulation for specific verticals
Environmental	• Better mapping and decision making regarding renewable energy • Efficiency improves resource and energy management

Figure 24. PESTLE Analisis

7.1.1. Political

Because of the implications of IoT in the use of personal data and the establishment of regulations for it within the context of the EU and its different policies around this topic, political factors play a role within national, European and global landscapes. For this reason, the concerns listed in Figure 24 play a role when analysing the macro-environment related to IoT.

Political factors are closely tied to legal factors but are more focused on the underlying drivers and the political process eventually leading to binding legislation [110]. In a report published in 2016, the global mobile trade body found that 60% of mobile users are worried about a world of connected devices, privacy (62%) and security (54%) are seen as the biggest threats worldwide, and home security raises

[110] https://www.databio.eu/wp-content/uploads/2017/05/DataBio_D7.3-PESTLE-Analysis_v1.0_2017-12-29_VTT.pdf

the most concern among connected devices and applications.[111] As for Brexit, the biggest impact lies within the negotiation agreements regarding access of the UK to the European single digital market[112].

7.1.2. Economical

As seen in the previous section, the landscape for the IoT development in economical terms is very positive. Most of the challenges in the landscape will be addressed in section 9. However, the main points that will require special attention are the ones regarding the labour and necessary skills, and the barriers to implement IoT. The former because 32% of Europe's workforce has insufficient digital skills, while 17% of the 15-29 year olds are disconnected from both employment and education. This will have an impact on the availability of skilled workers in high-tech industries andadvanced end users capable of taking advantage of high-tech solutions[113].

7.1.3. Societal

This particular section of the analysis is closely linked to the challenges from section 9.1. It is of particular attention to emphazise the points of scepticism and accessibility. The first one because Europeans feel that they are no longer in control of their data[114]. The second point because there is an unequal availability and access to IoT and in general new technologies, making it more common from large companies capturing and buying most of the smaller players across different verticals.

7.1.4. Technological

The European landscape presents a relatively mature market when it comes to data and connection availability. However, access can still be a key hurdle in some of the verticals, even if smartphone and internet penetration are greater than ever before. Several studies from Kearney show that Europe's high-tech industry in declining[115]. Europe is struggling to keep up with the rhythm of Asia and North America. The world's biggest technology companies nowadays like Amazon, Google, Baidu and Tencent, all originated outside of Europe.

7.1.5. Legal

Europe is definitely a global leader when it comes to the legal aspect of technology development and data protection. The GDPR is one of the key documents in this field, however, further challenges remain. The Big Data wave is coming as one of the key enablers of IoT, and it brings up new questions regarding the legal approach to be used in different new scenarios. For instance, there is a perceived violation of the international competition law since the smaller companies are not able to compete with big corporations which have more capabilities and resources. There is no legislation for information in case of mergers. And there is also a lack of legislation in terms of big data in some of the verticals, like the EU forest laws that directly affect the agriculture domain[116].

7.1.6. Environmental

Climate change and weather are one of the most pressing topics nowadays. In this case, IoT comprises an opportunity to actually help improve our understanding on these phenomena given its potential to create better mapping systems to make better decisions in terms of resource management. Besides this potential gain, the opportunity of improving efficiency and productivity will also impact in a broader aspect to the reduction of waste and needed resources.

[111] https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Digitisation-of-Ind-policy-doc-Nov-2016.pdf
[112] https://www.nortonrosefulbright.com/en/knowledge/publications/b5c7b5cc/impact-of-brexit-on-technology-and-innovation
[113] https://www.databio.eu/wp-content/uploads/2017/05/DataBio_D7.3-PESTLE-Analysis_v1.0_2017-12-29_VTT.pdf
[114] https://www.databio.eu/wp-content/uploads/2017/05/DataBio_D7.3-PESTLE-Analysis_v1.0_2017-12-29_VTT.pdf
[115] https://www.de.kearney.com/communications-media-technology/article?/a/rebooting-europes-high-tech-industry
[116] https://www.databio.eu/wp-content/uploads/2017/05/DataBio_D7.3-PESTLE-Analysis_v1.0_2017-12-29_VTT.pdf

7.2. Global competitiveness

The economic aspect is not the only reason why Europe should strive to maintain a leading position in IoT technology. In general, the strong technological base in the digital sector is of extreme importance for maintaining the competitive advantage on the global level from the economic and societal point of view as well as an adequate level of strategic autonomy. Digital technologies are shaping societal, political and geopolitical outcomes. Currently, the investment in R&D initiatives in the digital technology field are significantly higher in the US and in China[117], which puts Europe at a disadvantage. Therefore, it is of utmost importance to invest in promising projects related to European strategic interests and sovereignty, which will benefit Europe both from the economic and from the security perspective[118]. An advantage, which Europe can leverage on, is its prioritisation of and strength in social cohesion - an aspect contributing towards the adoption of new technologies. The EU share of global GDP is 22 percent and if we compare it to the share of European-based production of embedded electronics, with its 23 percent share of global production, it is well aligned. A leading domain of the EU is enterprise software (8 of the 20 world's biggest enterprises are headquartered in the EU) and mobile infrastructure. Nevertheless, the EU with its share of 6 percent lacks competitiveness in stand-alone electronic equipment, where the market is dominated by the US and Asia. With the spread of IoT, cloud computing becomes increasingly important, yet all of the five providers dominating the market (Amazon, Microsoft, IBM, Google, Alibaba) are based in the US or in China, leaving the EU behind[45].

7.2.1. European competitiveness

With the pressing insights from the global landscape, it is now important to understand where Europe stands in the different domains cited before and how these domains will be influenced by IoT. For that matter, the matrix of Kearney in Figure 25 shows a picture of where Europe stands in comparison to other regions. This matrix also sheds some light on which industries will be the most influenced, making the upper quadrants the industries of focus. The upper right corner shows the industries where Europe should place the priority to remain competitive. The upper left show possible areas where a new strategy can create big opportunities for Europe.

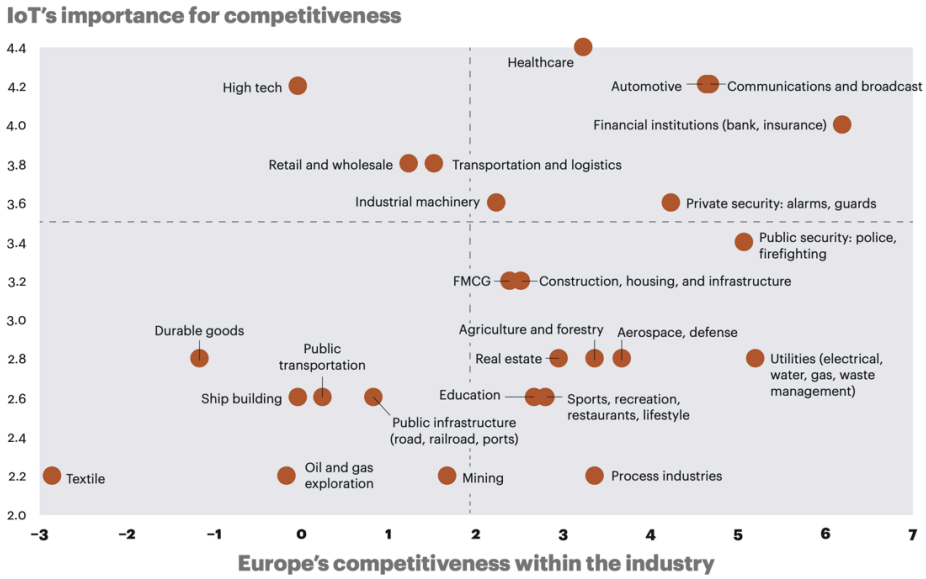


Figure 25 European competitiveness vs. IoT importance[119]

[117] https://www.mckinsey.com/~/media/mckinsey/featured insights/innovation/reviving innovation in europe/mgi-innovation-in-europe-discussion-paper-oct2019-vf.ashx
[118] https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf
[119] https://www.jp.kearney.com/documents/20152/435434/The%2BInternet%2Bof%2BThings-A%2BNew%2BPath%2Bto%2BEuropean%2BProsperity.pdf/abf7b3cc-333a-01bf-9089-3d2dde43564f?t=1493942640406

7.3. Input from the IoT community

An online survey was conducted from March to June 2019 to collect the views of the IoT community. 284 people from 29 countries (mostly European) took part in the survey[120]. The respondents primarily represent mostly companies (45 percent, of which 28 percent are SMEs and 17 percent industry) and research institutions (36 percent). Below, we provide a short indicative overview and concise description of survey results.

Security (including cybersecurity), privacy and safety (i.e. data protection) as well as interoperability are flagged as key priority topics for the next European research programme related to the Internet of Things. Next in line are artificial intelligence (AI), standards and technologies. Without doubt, security (including cybersecurity) is pinpointed as priority number one.

The respondents to the questionnaire would address as priority application domains of the European research and innovation roadmap smart cities & communities, health and mobility. However, other issues such as industry, energy, the environment and agriculture (including agri-food), are of high relevance. This makes it rather difficult, at this stage, to draw any further conclusions.

Within the identified application domains, the main issues to be addressed are by order of importance security (including cybersecurity), privacy and safety (i.e. data protection), the environment (incl. sustainability), interoperability and business models (incl. scalability).

When it comes to the most promising cross-cutting application domains of IoT, mobility and smart cities & communities stand out. Next come the environment (incl. sustainability), health, agriculture (incl. agri-food), energy and industry. It is therefore difficult, at this stage, to draw any further conclusions.

With respect to enabling a human-centred IoT, three priorities related to research and innovation seem to stand out: privacy and safety (i.e. data protection), humans/citizens, and security (including cybersecurity). In addition to those three main concerns, trust, adoption/acceptance and ethics also represent important priority needs.

For Europe to lead IoT technology and market adoption, action should be taken regarding legislation, business models (incl. sustainability), standards, adoption/acceptance, interoperability as well as cooperation/collaboration. Some respondents highlight Europe's struggle to 'foster true coordination and collaboration between R&D projects and initiatives' as well as a lack of 'focus on economic and industrial impacts' and 'people'.

To ensure transformation of research results into innovation and job creation, Europe should strengthen its legislative efforts to facilitate access to finance for SMEs, but also be more open to high-risk actions. One of the key challenges for the EU is to ensure sustainability of research results. Along with adequate business models, several respondents advocate for pilot actions (experimentation) in innovation ecosystems fostering cooperation/collaboration to encourage adoption/acceptance of new solutions. Cooperation/collaboration should be understood in a broad way, meaning not only academia and industry but also local governments and SMEs.

7.3.1. Survey: Top IoT application domains

When the respondents were asked to name three IoT application domains, the approximate distribution of the answers was as follows:

- 35% named Smart Cities (and Communities)
- 28% named Health
- 19% named Energy
- 15% named Agriculture

[120] 78% of responses came from EU countries, in particular, in order of importance: Spain, Greece, Belgium, Denmark, Germany, Italy and Sweden.

- 15% named Industry
- 13% named Transportation
- 12% named Environment

When the respondents were asked to name **cross cutting IoT application domains**, the approximate distribution of the priorities was:

- 34% prioritised Smart Cities (and Communities)
- 21% prioritised Health
- 19% prioritised Transportation
- 11% prioritised Agriculture
- 10% prioritised Environment
- 10% prioritised Mobility
- 8% prioritised Buildings

From these results it is important to point out that the domains of Smart Cities and Health are considered not only the ones being on top of mind of most of the respondents, but also the ones considered to be where IoT has more untapped potential in the European landscape. It is interesting to see that when compared to the global share of IoT projects in Figure 7, Smart Cities and Health occupy in both the top positions, however, Industry does not seem to be present in the survey results as a priority.

7.4. Context by Industry Domain

Based on both rankings of importance, a brief description is added on Europe's context on each of the main industries. The potential opportunities in economic terms and potential developments can be found in the next chapter.

7.4.1. Smart Cities

Europe is one of the leaders in terms of smart cities, with over 12 of the top 25 cities of the IESE cities in motion index[121]. This great positioning responds to Europe's early efforts to overcome the challenges of developing smart cities through several initiatives aligned with their Europe 2020 targets. By promoting policies and programs aimed to develop smart cities in a coordinated way[122] and solving funding needs by private public partnerships[123], the EU has managed to quickly develop their "Lighthouse" cities and aims to have over 300 smart cities by 2020[124]. Today, Europe counts with various programs constantly reinforcing its Smart City development, from the success of the SynchroniCity LSP project[125] to the centralization and clusters of European Innovation Partnership on Smart Cities and Communities (EIP-SCC)[126].

7.4.2. Health

Europe faces the trend of ageing population more than ever[127]. Although the region keeps a strong position in this industry, it is not so easy to see how the different players are embracing change. For this industry this is crucial, since, as shown in Figure 26, Healthcare is an industry where IoT is vital for competitiveness. As one of the clusters of global challenges and European industrial competitiveness, healthcare is a top priority, with areas of intervention going from tools, technologies and digital solutions, to personalised medicine and medical systems improvements[128].

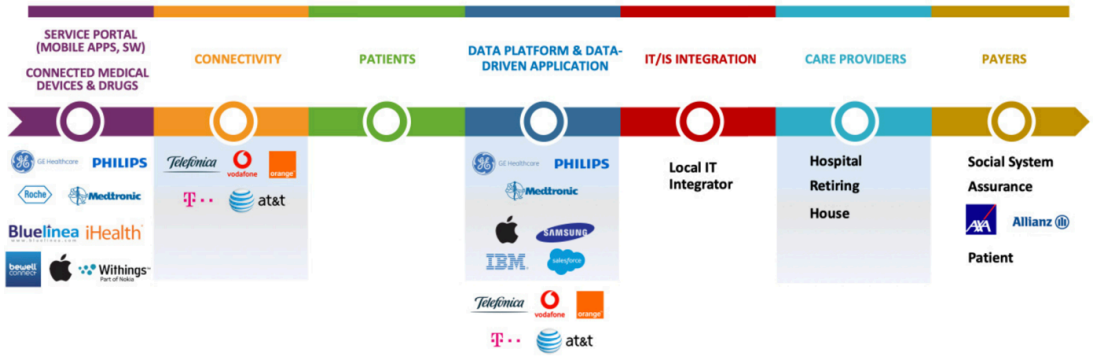


Figure 26. Healthcare Solutions Value Chain

[121] https://www.ieseinsight.com/doc.aspx?id=2124&ar=&idi=2&idioma=2
[122] https://www.itu.int/en/ITU-T/climatechange/resources/Documents/MappingSmartCitiesinEU-2014.pdf
[123] https://www.osborneclarke.com/media/filer_public/b3/bc/b3bcaffa-2b02-465d-804d-af85d735e8e9/smart_cities_in_europe_e-version.pdf
[124] https://energypost.eu/europe-aims-to-have-300-smart-cities-next-year/
[125] https://synchronicity-iot.eu/wp-content/uploads/2020/01/SynchroniCity-guidebook.pdf
[126] https://eu-smartcities.eu/page/european-context
[127] https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf
[128] https://ec.europa.eu/info/sites/info/files/research_and_innovation/strategy_on_research_and_innovation/presentations/horizon_europe_en_investing_to_shape_our_future.pdf

7.4.3. Transportation

With its strong mobility industry, Europe stands as an important voice when it comes to smart transportation. Starting with solutions like Asset & Fleet management and Freight monitoring in the ground transportation sectors, to Airport optimization and Passenger traffic flow, the transportation sector is an area where Europe is leading the way[129]. In the Transport sharing area, Europe also stands out with numerous bike sharing, car sharing and other services across different cities. Lastly, many European cities have already integrated smart solutions in their public transportation systems, significantly improving the quality of this service.

7.4.4. Manufacturing

Having invested at higher levels than their competitors in other region, Europe leads the way in Industrial IoT, moving to scale faster with three times more implementations than in the US [130]. On a country specific look, Germany paves the way with the automotive and manufacturing sectors leading the adoption rate, driven by mid-market companies[131]. In Gartner's study[132], Software AG outstands as a visionary IIoT platforms headquartered in Germany, amongst other global players. Followed by the UK, France, Italy and the Nordic and Eastern European markets, the trend is passing from leveraging Industrial IoT to develop new services and solutions, to generating efficiencies and cost savings. All across Europe are also implementing IIoT related activities and even strategic alliances like ADAMOS are being established to accelerate the development[133]. Although Europe leads the way in this domain, security and privacy, remain an important preoccupation and a barrier to widespread adoption. Bain also estimates that mastering these areas promise giving European IoT providers a substantial competitive advantage[130]. Another important challenge for this domain lies on the high-tech industry side, where several studies from Kearney show that Europe's high-tech industry in declining[134]. Europe is struggling to keep up with the rhythm of Asia and North America. The world's biggest technology companies nowadays like Amazon, Google, Baidu and Tencent, all originated outside of Europe.

7.4.5. Telecommunication

Although this industry didn't rank as one of the priorities from the survey, it is important to point out that Europe has a sophisticated infrastructure that is the backbone of the IoT development. Companies like Orange, Telefonica and T-Mobile have adopted LTE technologies and will most probably continue their strong investments that enable the IoT penetration[135]. This gives Europe a leadership position.

[129] http://publications.europa.eu/resource/cellar/35f3eccd-f7ce-11e5-b1f9-01aa75ed71a1.0001.01/DOC_1

[130] https://www.bain.com/contentassets/325cb60011ee4cbd8891381ec5ed781e/bain_brief_europeans_extend_their_lead_in_the_industrial_iot.pdf

[131] https://www.cbi.eu/market-information/outsourcing-itobpo/intergrated-internet-things/market-potential#which-european-countries-offer-most-opportunities-for-iot-services-outsourcing

[132] https://b2bsalescafe.files.wordpress.com/2019/09/gartner-magic-quadrant-for-industrial-iot-platforms-june-2019.pdf

[133] https://www.smart-industry.net/iot-readiness-is-europe-up-to-it/

[134] https://www.de.kearney.com/communications-media-technology/article?/a/rebooting-europes-high-tech-industry

[135] https://www.jp.kearney.com/documents/20152/435434/The%2BInternet%2Bof%2BThings-A%2BNew%2BPath%2Bto%2BEuropean%2BProsperity.pdf/abf7b3cc-333a-01bf-9089-3d2dde43564f?t=1493942640406

7.5. Context by Priority Topics

Based on the community's ranking of importance, follows a brief description on Europe's position in the most pressing topics. The potential opportunities in economic terms and potential developments can be found in the next chapter.

7.5.1. Security and Cybersecurity

With the presence of the European Union Agency for Network and Information Security (ENISA), Europe leads the way in terms of cybersecurity. ENISA sets the scene and coordinates by guiding the implementation of a coherent framework of IoT cybersecurity[136]. Together with projects like SerIoT, SecureIoT[137] and C4IIoT[138], Europe stands at the forefront in terms of cybersecurity.

7.5.2. Privacy

Also, at the forefront with projects like GHOST[139], supported within the context of Horizon 2020, Europe aims to bring privacy as a standard across the different domains. To achieve an implementation that better suits each domain, different projects are being implemented to cover the details in every industry[140].

[136] https://www.digitaleurope.org/resources/defining-the-way-forward-for-iot-security-and-certification-schemes/
[137] https://ec.europa.eu/digital-single-market/en/blogposts/fighting-cybersecurity-eight-new-eu-funded-projects-more-secure-iot
[138] https://www.c4iiot.eu/
[139] https://www.ghost-iot.eu/ghost-project
[140] https://www.researchgate.net/publication/329070695_IoT_European_Security_and_Privacy_Projects_Integration_Architectures_and_Interoperability

8. INTERNET OF THINGS (IOT) ECONOMIC OPPORTUNITIES AND VALUE CREATION

This section is partly taken from the NGIoT Scoping Paper with several enrichments, it contains a general assessment of the economic impact of IoT as well as a description of the opportunities present globally and in the recognized domains from the survey in order of importance for the European region.

8.1. Micro- and macro-economic impact

IoT influences the economy on both the macro- and micro-economic level. From the macroeconomic perspective, a good proxy for investigations is needed. As a proxy for investment in IoT, the number of machine-to-machine (M2M) connections can be used. It has been shown that a 10 percent increase in M2M connections translates into an annual increase of 0.7 percent, 0.3 percent and 0.9 percent in GDP, services GVA (gross value added) and industry GVA, respectively[141] (calculated on a sample of 27 countries in North America and Western Europe). Therefore, an economy with more investment in IoT is likely to observe an increase in trade surplus.

The implementation on IoT across several domains will have significant implications on the micro-economic level. Due to the increased availability of measurements, data collection and transfer in a dynamic setting, mathematical algorithms will be developed to enhance further a sophisticated decision making. The effective handling of big data is of utmost importance. In fact, this will lead to noticeable cost savings, reduction of waste, transformation of the cost of asset ownership, better capital allocation and overall increase of efficiency. Furthermore, real-time, automated decision capabilities can be developed on top of that. All this will create significant value at the micro-economic level, as this will help with more efficient operations and thus increase profitability. It is within this dimension where the introduction of IoT can create a significant value for companies that will have strong incentives to introduce IoT related systems not only for increased efficiency but for its enormous potential to distinguish them from the competitors.

However, a potential caveat surges given the possible exclusion of SMEs from IoT systems implementation due to the initial cost upfront. Although the implementation of IoT generates benefits, the question might be which stakeholders will harvest the benefits from the IoT implementation (e.g. making data available). Sometimes, the costs for installing sensors are borne by SMEs, who consequently do not capture the added value from the measurements since most of this value come from the processing and interpretation of this data, which generally have a significant extra-cost.

A transformation of the job market is also expected. Some routine, less-qualified jobs are likely to disappear. However, IoT technologies will create a dire need for certain experts, such as big data scientists, engineers, IT specialists and others. With the extended digital skills of the European workforce, new organizational challenges will occur because of new ways of working and collaborating enabled by the new technologies.

The transformation of the current economy due to IoT could lead to the extensive inclusion of crowdsourcing/-funding, outcome economy and circular economy models. Because of the added benefits of these models, ideally, the new system should focus on lowering the barriers to entry and enhance an open-market opportunity with equal opportunities and minimal barriers.

[141] https://www.frontier-economics.com/media/1167/201803_the-economic-impact-of-iot_frontier.pdf

8.2. IoT Potential and Opportunities

So how exactly can this economic impact be realized in the upcoming years and what are the opportunities that have the most potential nowadays? Untapped potential of IoT can be found on a wide range of areas, going from the effective allocation of resources and empowerment of citizens in Europe. However, some of these opportunities are closely tied to the development of IoT enablers (connectivity options such as WIFI, 5G, Bluetooth, then cloud services and analytics), which should be well aligned with the development of IoT. Irrespectively of this, the landscape as of now shows that the continued growth of the IoT industry is going to be a transformative force across all organizations.[142]. For this reason, the analysis based on the survey segments the potential across the different domains on the following section.

8.2.1. Standardisation in IoT

Taking into account the estimated growth of the IoT ecosystem, standardization will play a more important role. Until now firms have been building their own strategies and solutions with a wide range of platforms and technologies and therefore one of the consequences is the fragmentation of the technological solutions which may also result in a fragmentation of the market. Standards represent an essential part of the organization and functioning of modern socierty including ICT and information security. In the case of IoT technologies one of the consequences of an unstandardized IoT is that many devices are not “plug and play” ready. In many cases end-users must download software and drivers to make them work with existing technologues. If one of the goals, also for the Digital Single Market, is to facilitate the spreading of and access to technology there is a need to make it easier to use. Standards can play an important role in this context by promoting best practices, integration and interoperability of systems, privacy and security requirements.

8.2.2. The creation of value and the IoT trust framework

In order for facilitate the growth and development of the IoT market and of the value chain a fundamental element is the adoption of a “trust by design” approach. We have already seen in the section devoted to societal challenges why the protection of security and privacy need to be built as a key feature in IoT deployments. As regulation is fragmented along national lines different stakeholders have taken an initiative for the creation of an IoT trust framework to raise the level of security of IoT devices and related services. The framework developed covers different areas focusing on the following principles: authentication, encryption, security, updates, privacy, disclosures, control, communications. The framework identifies core requirements that manufactures, service providers, distributor/purchasers and policy makers need to understand and embrace to develope a trust framework for the IoT[143].

8.2.3. IoT and the Digital Single Market

IoT deployments and devices represent a building block of the digitisation of our society and economy, a context into which people and objects are interconnected through communication and networks. The Digital Single Market Strategy[144] adopted in 2015 already included elemets for consideration of a European approach to the IoT. The strategy adopted by the European Commission underlines the need to avoid fragmentation and foster the interoperability. The document published in 2016 “Advancing the Internet of Things in Europe” has specified the EU vision based on threee pillars: 1) a thriving IoT ecosystem; 2) a human-centred IoT approach; 3) a single market for IoT. All these pillars, and their strenghtening have a market relevance both internal and external for the EU. The pillars need to be bases on a sustainable ecosystem development, the promotions of common standards and the need to look at societal challenges posed by IoT developments. The “European data economy” will need to propose solutions that facilitate the free flow of data among European countries and rules concerning liability issues in complex environments in order to enhance legal certainty and trust in complex

[142] https://www.businessinsider.com/internet-of-things-report?IR=T
[143] The documenti is available here: https://www.internetsociety.org/resources/doc/2018/iot-trust-by-design.
[144] TDB

environemnts such as the IoT one. According to the European Commission the value of the data economy will increase to EUR 643 billion by 2020 representing 3,17% of the overall EU GDP.

8.2.4. 5G and IoT

The transition of many companies and organizations to the Internet of Things will also be based in the adoption of key technologies such as the fifth generation of wireless technologies (5G). 5G offers to firms important benefits in terms of data speed, latency, reliability, efficiency, capacity and security. 5G is therefore expected to support a wide array of new solutions. As highlighted by KPMG: "Some of the benefits of IoT could be realized within an existing telecommunications infrastructure, but previous wireless technology generations do not have the capability to integrate with autonomous robots or advanced technologies. In contrast, when IoT is combined with 5G networks in a transformation strategy, the goals of i4.0 come within reach"[145]. The deployment of 5G will therefore constitute a building block of the digital single market and the European Union has already taken several initiatives already from 2013 by establishing a Public Private Partnership on 5G (5G PPP) and by funding several research projects. 5G standards are also one of the five priority areas under the European industry initiative[146]. The 5G Action Plan for Europe[147] was adopted in 2016 with the goal of starting the deployment of 5G services in all the EU Member States by the end of 2020. Given the market relevance of 5G deployments the European Commission launched also the European 5G Observatory in 2018 to monitor major market developments in a global context. For the development of proper market solutions, the role of Member States has to be taken into account as well, for this purpose a report on national strategues and their consideration under a European perspective has been published[148]. 5G deployments are to be considered in a market perspective also from a security and geopolitical, for this reason a coordinated risk assessment was undertaken.

8.2.5. Open Innovation role

A fruitful interaction between IoT growth and the role of open innovation could bring new opportunities and innovations to companies and to society. Open Innovation, like the IoT brings in a more distributed and connected approach. In fact, with its reliance on open source/open data/ open standars it changes the propietary paradigm of research and development that characterizes many companies. Open Innovation contributes to companies looking beyond their boundaries to seek and utilize inflows and outflows of knowledge. To this extent the value created thourgh data collection and data analytics by IoT deployments can be one on of the most important tool of a new approach.

8.3. Sectorial Analysis – Opportunities per Application Domain

There are several domains, where there are opportunities for the best exploitation of IoT technologies from an economic perspective[149]:

- Agriculture and Smart Farming: IoT technologies enable drop control, remote monitoring of livestock, data collection about soil, crop and cattle conditions and it **reduces human intervention** (and thus labor costs) in favour of automated farming. Also, data analysis helps **optimize farming and hence save costs and/or increase revenues.**

- Healthcare: the introduction of IoT in healthcare supports hand hygiene monitoring systems, **remote health monitoring through wearable devices and smart medical apparatus manufacturing.** The combination of smart sensors and cloud computing is used to **optimise the flow** of patients, staff, equipment and medical supplies hospital wide. This gives many opportunities for

[145] KPMG, *Converging 5G and IoT: a faster path to smart manufacturing*, available at: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/06/converging-5g-and-iot-a-faster-path-to-smart-manufacturing.pdf.
[146] TDB
[147] TDB
[148] TDB
[149] https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf

extension of revenue streams in the healthcare industry. Due to optimization based on dynamic data, it **can reduce inefficiencies** and enable **better allocation of financial resources. Biometric wearables to track health and lifestyle** provide important information concerning the tailored medical treatment as well as **solid data for health insurance companies.**

- Energy Management: IoT technology can be employed to create **smart grids that price and route power, based on the demand and prevent blackouts.** This leads to optimization of resources and **better service.**

- Manufacturing: IoT can be used in manufacturing for **predictive maintenance of machinery** based on the sensor data collected. These further leads production line monitoring with sensors to **optimise equipment utilisation**. IoT implementation would also help manufacturers increase **business profitability and productivity** of both humans and machines, by **streamlining production processes and automating plant machinery** with RFID chips that **store product configuration data, work instructions & work history**. **Predictive analytic**s engine help to make the future manufacturing plants more **autonomous** in terms of predicting and fixing potential disruptive issues, which might lead to significant losses.

- Media: IoT supports **hyper-personalised advertising** to drive relevancy and **effective targeting,** hardware sensors can measure and analyse metrics such as high footfall timings, popular store sections and products, whilst also targeting consumers with push marketing messages based on their **individual purchasing habits**. This can remarkably increase sales, while the cost of the implementation of IoT technology is relatively low. This boost profits.

- Insurance: the implementation of IoT across several domains and c**ontinuous data collection and evaluation leads to new models of risk assessment** (including a user's credit & claims history, and the size and type of property owned etc.). The **risk models are highly personalised** and data-led and data from several connected devices are analysed (wearables, smart home appliances and connected cars used by the policyholder etc.). This helps insurers to **monitor the policyholder's personal habits and behavioural preferences and develop better models effectively assessing the insured risk and offering added value**. Yet, this brings major challenges in terms of **ethics and privacy.**

- Transportation: **predictive maintenance, traffic jams predictions, optimal route calculation** and car tracking are one of the ways of utilization of IoT in transportation which lead to cost saving. Mobility as a service stands as a tremendous opportunity to create value in the public transport field[150].

- Smart cities: one of the domains, where IoT has an enormous potential. Monitoring and managing traffic and transportation systems, power plants, **water supply networks**, **waste management, buildings, community services** and others provides a solid basis for analysis and predictions, thus enabling cost optimization and effective allocation of resources.

[150] http://publications.europa.eu/resource/cellar/35f3eccd-f7ce-11e5-b1f9-01aa75ed71a1.0001.01/DOC_1

9. IO INTERNET OF THINGS (IOT) CHALLENGES

Some of the IoT related challenges where mentioned briefly in the PESTLE analysis, however, to fully grasp the notion of the most pressing issues in the IoT landscape, this section provides at first a description of most pressing economic challnges(E), followed by the main research challenges (R), their value-added and the necessary steps needed to enable the capture of this value.

9.1. Key economic and policy challenges

The implementation of IoT does not only provide good opportunities for economic exploitation, but also brings along new challenges. The present paragraph provides an overview of the most important challenges in the IoT domain from an economic and policy perspective:

- **Support for SMEs and start-ups (E1).** SME enterprises in Europe play a significant role in the economy, thus Europe needs to ensure their smooth transition towards innovative solutions, including IoT technologies. The adoption of IoT may bring a lot of added value to companies and it may give them a certain competitive advantage. Companies which will not be able to adopt IoT appropriately might suffer and later also disappear from the market. Small players often face the problem of capital barriers to enter the market as well as lack of recognition and trust, as they cannot use a strong and well-established brand (e.g. like Amazon, Google etc.). Additionally, it is crucial to support start-ups (e.g. providing access to business angels, investors, VC funds, accelerators, supporting partnerships with big players within that industry), as start-ups have the capacity to disrupt the market and to push innovation into new sectors in agile ways. However, it is not easy to find attractive IoT startups. Most of IoT startups fail to show a substantial recurring revenue stream, their revenue is often based on project-based consulting fees or through the support of one-time proof of concept (PoC) implementations rather than highly scalable software[151]. Supporting SMEs and start-ups can be rather difficult because of this, but it is still the best alternation for Europe to limit market monopolisation by the major and well-established players and at the same time strengthen European innovation in IoT domains.

- **Accurate economic parameters estimate (E2).** Currently, it is very challenging to estimate the key parameters used by investors in their decision-making process. Specifically, investors are interested in the return on investment estimate (ROI), revenues, costs, profits and risk profiles of investments in IoT. In this regard, looking at trends and past investments in innovative technology solutions could provide guidance.

- **Data and information as critical assets (E3).** The key value of the data gathered from IoT devices is not the data itself, but the information which can be extracted from the data. In order to price data, it is necessary to have a better understanding of data management, interoperability and standards, services provided around the data (security, protection, etc.), data ownership and accountability, ethics, and how they can influence the future value of data. In addition, questions to take into account include the potential connectivity partners have to monetise the data, the size of the market, market accessibility, market entry barriers, and competing data providers and services.

- **Increase of digital skills and competencies (E4).** The implementation of IoT will require a significant number of skilled workers in IT, computer science, big data science, artificial intelligence and other related technologies. This requires not only the development of study programmes at bachelor,

[151] https://iot-analytics.com/iot-investments-m-and-a-market-update-2018/

master and PhD levels, but also on a professional basis to regularly update employees and professionals already in the work process through tailored courses, workshops, interactive trainings, etc. An important target group is children and adolescents - children should be educated about technology from primary school and supported to choose a career in technology-related domains, removing current gender gap barriers.

- **Build Trust (E5).** Building trust among current and potential IoT users, policy makers and citizens is essential for the successful adoption of IoT. The technology adoption curve could be an inspiration, including learning from early adopters, building trust on both supply and demand side and changing mind-sets to support technology implementation. Other initiatives aiming at building trust may include raising awareness through success stories and building trust through transparent guidelines and frameworks that address the ethical and privacy implications of IoT. Educating people on the value data can bring to their everyday lives and helping to achieve sustainability goals are also important steps towards improving trust with regards to IoT implementation. However, the key questions are how to make individuals and enterprises trust IoT technologies sufficiently to change their habits and processes for the better; and how to prepare organizations for the inclusion of IoT technologies? Behaviour change requires the right attitude, which makes it a complex goal.

- **Identification of the Key Regulatory and Legal Issues (E6).** New technologies entail legal and regulatory issues. The most important regulatory and legal issues and open questions related to IoT should be identified and gaps and controversial open questions need to be solved in a transparent and agile way. A point that should be highlighted is the speed of the new regulations. Having the regulations at the right time is very important for optimal exploitation of IoT; otherwise, investors will be reluctant to invest in new IoT-related technologies and businesses, as they may face a serious risk of their investment objective not being approved.

- **Interoperability and Replicability (E7).** IoT technologies will generate huge amounts of data. Data can only attain its true value when it can be shared and monetised across domains, frameworks, shareholders and countries. For that reason, common harmonised data models should be adopted. Following harmonised data models, harmonised functionality should be focused on. An example could be the harmonised implementation of some open source components, in particular the FIWARE context broker that is specifically enabling the vision towards a system-of-systems approach to facilitate interoperability and expansion. Another example is the Open & Agile Smart Cities network which connects 140 smart cities in 29 countries globally and strives to establish the Minimal Interoperability Mechanisms (MIMs) that are needed to create a market for smart cities and IoT. MIMs are simple and transparent mechanisms, ready to use in any city, regardless of size or capacity. By implementing MIMs, cities increase the speed and openness of innovation and development, whilst decreasing cost and inefficiency. MIMs allow cities to engage in global digital transformation, addressing the lack of convergence of standards. IoT solutions must be interoperable and replicable, which requires orchestration of business processes, effective collaboration and practices. This might require more technologies than just data and information interoperability (e.g. TM Forum develops services and technology agnostic operational management APIs and testing capabilities). The effective integration of cross-domain data in business and organizational processes is another aspect.

- **Security and Reliability by Design (E8).** In order to work on the above points, we must ensure the security and reliability of the technology solutions. One potential caveat could be to ensure that with increased workload, scalability is also ensured to remain reliable.

- **Innovation procurement (E9).** Ensure that public procurement is well aligned with the dynamics of IoT and the consequent changes in the IoT applications. The emphasis must be put on the cooperation of public administrations in Europe with the aim to encourage first movers and estimate appropriately associated risks. As a benchmark, successful procurement strategies from the past can be used. However, the current public procurement has a clear preference towards long-standing companies and does not support the 'try before you buy' model. A key element is to develop trusted KPIs and certification schemes, linked to broader initiatives such as DESI-local and the UN SDGs.

- **Sustainability (E10).** Ensure sustainability related to the increasing number of new technologies, materials for sensors, electronics and power source.

- **Cohesion (E11).** Focus on bridging the smaller and rural communities and developing areas also, not just the innovation and economy frontrunner territories. There are interesting business opportunities in developing countries.

- **Sovereignty (E12).** Ensure Internet sovereignty, as IoT is based on the Internet. Although data sovereignty could be solved by data centres in Europe, there is a significant dependency on non-European cloud infrastructure and data are also handled by non-European service providers.

9.2. Priority research challenges

By analysing the above sources and taking into consideration the latest disruptive technologies, NGIoT identified the following high-level research challenges for the next work programmes. Priorities identified cover different aspects of the IoT stack and, accordingly, relate to other transversal research and technologies, including: 5G, Distributed Ledgers, Big Data, Artificial Intelligence, Cyber Security, and Cloud Computing. Some of the priority challenges go beyond pure technological research and require a holistic approach to take into consideration research in sociology, anthropology, economy, neurology, biology and ethics. So, while NGIoT recommends priorities to be included in the future relevant work programmes, not all of them need to be covered in an IoT specific objective.

9.2.1. Foundational challenges

- **Reliable, low-cost, sustainable and scalable IoT networks (R1).** While LPWAN solutions have been largely tested and offer a low-cost solution for large IoT deployments, they suffer several drawbacks in terms of supporting real-time and high-bandwidth scenarios. Despite the fact that NB-IoT and LTE-M appear to be initial solutions to the open challenge, they fail in some respects. On the one hand, NB-IoT, designed with increased reach and lower cost and power consumption, offers limited bandwidth and latency around 1 sec. On the other hand, LTE-M, while providing higher bandwidth, fails on the low-cost constraint. This implies that the road to provide large-scale deployment, able to support real-time scenarios with bidirectional communication at a low cost, is still a challenge. 5G and its evolution should go further to address the low cost, massive device deployment. Such technologies need as well to be sustainable by limiting the usage of resources and the impact on the environment, to avoid the large-scale deployment of devices becoming unsustainable from an environmental point of view. The forecasted increasing number of devices we will witness in the future will make this challenge more pressing. This challenge relates to optimizing IoT integration into the global Internet, with a focus

on IPv6, as well as in cellular networks, such as 5G (and other future networks), but it entails as well research in relation to energy and sustainability of IoT devices.

- **Next Generation IoT data processing architectures (R2).** The Internet of Things (IoT) is one of the key drivers of the Big Data phenomenon. IoT was one of the main drivers for the switch from batch analytics to real time analytics solutions. Still, while a plethora of real-time processing solutions and platforms are available today on the market, it is clear that the amount of data generated is growing faster than the processing capacity, and often poses a real challenge to the storage capacity. This hinders the ability to generate value from sensors data in real-time and also as batch processing, given that it is not always possible to retain and store all the generated data. Current research and development trends to solve this challenge focus on the so-called edge computing architecture. This architecture solution, while it is able to cope with today's needs, applying the 'divide et impera' principle leveraging existing data processing solutions, may not be enough for future needs. Most probably, real-time analytics architectures will need to be retaught, and their functions - to increase their speed - will need to be directly available at the level of processing units (this trend is already being explored by some activities in the FPGA research). In short, IoT data processing architectures need to be scalable by design. This challenge relates mainly to Edge Computing, Distributed Ledgers, Big Data, and Artificial Intelligence research.

- **Futureproof security and trust (R3).** While there is a plethora of past and ongoing research on security in the IoT field, the constant and rapid evolution of IoT technologies and cyber-attacks, requires consistent investment in these areas. In this respect, research should focus on 'intelligent' approaches to the security, i.e. on the ability to 'learn' new attack patterns and derive counter solutions autonomously. Beyond cyber security for IoT, trust toward IoT solutions and data generated by devices is becoming an important trend in the market. Solutions are focused on providing ways to produce and consume IoT data by highly decentralised and loosely coupled parties through secure traceability mechanisms such as blockchain. Still, current blockchain solutions are far from tackling scalability requirements posed by real-time data scenarios in several IoT market segments. It is important to highlight how trust is an essential aspect for the human interaction with IoT-enabled services, and goes beyond pure technological aspects, encompassing also psychology, sociology and ethics research. This challenge relates mainly to Distributed Ledger, Artificial Intelligence, and Cyber Security research.

- **IoT, processes, and data Interoperability (R4)**. While eventually, as in other technology fields, some standards (de facto or actual) will finally prevail regarding integration among devices and platforms, data interoperability will remain a challenge, that, while it may be mitigated by effort in the harmonisation of data models within single domains, will still be present when dealing with legacy systems and cross-domain data exchange. This would result in increasing costs on the integration of IoT solutions. While several technologies promised automated semantic interoperability in the past, this is still far from being achieved. Still, a pragmatic approach, where semi-automatic interoperability is achieved through limited human interaction, seems possible with today's technologies. While data interoperability is a requirement to enable cross-domain applications, an even more complex aspect that requires attention is the ability to orchestrate business processes across domains. Processes enacted within IoT and data platforms may be much more complex to interoperate than data, thus, enabling the interoperability between cross-domain platforms requires solutions beyond data interoperability. Past research in the field, e.g. semantic business processes, showed little scalability and applicability - novel

scalable and reliable solutions are required. This challenge relates mainly to Artificial Intelligence research.

- **IoT, Citizens, Privacy-by-design, and Ethics (R5).** While most of the challenges discussed above have a primary focus on technology, there is an important challenge unrelated to technology that needs proper attention for the development and adoption of Next Generation Internet of Things solutions. It is clear that the wider the adoption of IoT, the wider the 'intrusion' of devices and 'intelligent' services will be in our everyday life. What is an acceptable level from a citizen's perspective? What are the ethical implications that Next Generation Internet of Things solutions need to face? How it is possible to make what happens behind the curtains more transparent to ensure that intelligent solutions can be trusted? How can such solutions ensure compliance with GDPR, as well as with future regulations in this field? How can citizens be truly aware of the decisions they are making within respect data processing? How can we ensure an inclusive approach to IoT and counteract possible inequalities that might emerge with the wide adoption of IoT? And as connectivity intensifies, citizens will increasingly request spaces of disconnection. How can we facilitate these requests? This challenge is clearly demanding for a multidisciplinary approach embracing legal, sociological and ethical research in relation to the adoption of IoT and connected technologies, such as Artificial Intelligence.

9.2.2. Emerging challenges

- **Real time decision-making for IoT (R6).** While a plethora of solutions are available for deriving knowledge from data, IoT poses a new level of challenges to machine learning and its recent evolutions (the so-called deep learning wave). Coordinating real-time decision-making based on a widely distributed and decentralised infrastructure, so as to achieve a common goal, is not trivial. Despite being not trivial, this ability is a key enabler for different scenarios that are becoming more and more relevant for the market, like in the use case of self-driving cars. In several of these scenarios, decision-making will also need to take into account the 'human' factor, and the underlying ethical aspects, including the obstacles that lack of trust may pose to such solutions (which is a general concern in AI-related research). This challenge relates mainly to Edge Computing, Big Data, and Artificial Intelligence research, but also encompasses ethics, socio-economic and psychology research.

- **Autonomous IoT solutions (R7).** Maintaining an IoT infrastructure, spanning from the platform to the sensor layer, is a complex task. While nowadays there are a plethora of solutions helping resource orchestration (relying on the development of principles largely adopted by cloud platforms), the room to increase automation is still large at each level of the stack. Beyond that, autonomous IoT systems may be able to transform C-level KPIs into corresponding actions at the different layers of the IoT stack, thus reducing time to implement C-level decisions. In this sense, the most promising trend is the adoption of novel Artificial Intelligence techniques in combination with latest virtualisation trends proposed by 5G research to ensure a higher-level degree of self-automation by IoT technologies, from the sensors through the transport network, the gateways and up to the platforms. This challenge relates mainly to 5G, Edge Computing and Artificial Intelligence research. Another correlated challenge comes from the maintenance cost of IoT deployments, which is directly linked to the energy efficiency and autonomy of IoT solutions.

- **Human and sustainable development in the loop IoT (R8)**. While several IoT and CPSs solutions are intended to serve humans, most of the IoT solutions we witness today are still designed for M2M communication. Thus, the support for interaction with humans, and the enablement for them

to take decisions and interact with the systems is often limited. While we have witnessed the usage of humans as "sensors", most of the existing solutions still consider the human as an external and unpredictable element to the IoT system control loop. Research in the direction of including the human element in IoT technologies is key and should take into consideration human intents, psychological states, emotions and actions inferred through sensory data. In this respect, also the research on the Digital Twin concept will have a key impact, enabling humans to perceive IoT systems more related to their physical counterpart. This challenge is clearly demanding for a multidisciplinary approach combining Artificial Intelligence, ethics and psychology research. Similarly, IoT can play an important role in achieving sustainable development, including the UN Sustainable Development Goals (SDGs).

- **IoT data sharing and monetisation enabling models and technologies (R9)**. While different IoT Data Markets are starting to go live recently, their appeal in the market still seems limited. This is mostly due to two factors: i) the scale of the available data in these data markets that is often limited and hence only of interest for a limited set of stakeholders; ii) the actual value of the data on the market, that being mostly raw data, has limited value for potential buyers. The first issue is mainly driven by the fact data owners are not motivated to share data for different reasons: e.g., a loss of data control, lack of adequate incentives, and a lack of trust toward intermediary platforms. The second issue is related to the fact that most of the platforms, not having enough data in place, cannot offer actual added value on top of the raw data provided by data owners. Latest trends in the data-sharing technologies show how Distributed Ledgers can increase trust toward data sharing and increase the feeling of data control by owners. This challenge, despite its relation to different technology fields, is mostly a socio-economic challenge related to the development of proper business models fostering the creation of larger IoT Data Market.

According to the initial outcomes of the survey, the most important high-level topics for the IoT research and innovation agenda for 2021-2027 are:

1. IoT security, related to R3.
2. IoT privacy and data protection, related to R5.
3. IoT interoperability, APIs and Standards, related to R4.
4. IoT and Artificial Intelligence, related to R6 and R7.
5. IoT & society (including sustainable development), related to R1 and R5.

9.3. Key challenges per domain

Because it is of the interest of this study to show a linkage between the identified challenges and the needed research to enable the value-added in their respective domains, the table below summarizes the main points concluded from the analisys.

Domain	IoT Challenges & Value-added	What is needed
Agriculture and Smart Farming	**Challenges**: IoT adoption in Smart Farming is still limited. This is mostly related to the costs of the infrastructure and to benefit not yet clear. **Value-added:** predictors based on IoT data can play a fundamental role, but they demand for large amount of data to be available	• Reliable, low-cost, sustainable and scalable sensor networks (R1) • Incentive to make data more available • Real time decision making for IoT (R3) • IoT Data Sharing and Monetization enabling models and technologies (R7)

Healthcare	**Challenges**: health data are sensitive data, this poses a number of ethics, privacy, trust and security questions on IoT solutions **Value-added:** a better evolution of IoT technologies in the medical field, especially within respect their interaction with the human factors, can revolutionize the healthcare sector.	• IoT, Citizens, Privacy & Ethics (R9) • Future proof trust and security (R5) • Human in the loop IoT (R6)
Energy Management	**Challenges**: Not yet available models for sharing and accessing data across the different stakeholders in the energy market. **Value-added:** The ability to optimize in real time energy resources is key.	• Real time decision making for IoT (R3) • IoT Data Sharing and Monetization enabling models and technologies (R7)
Manufacturing	**Challenges**: the cost for large deployment of sensors (as needed by complex production plants) and the complexity of managing such sensors and data coming from them, constitute an entry barrier (smart manufacturing requires the integration of a plethora of different data sources and providers). Security and trust have a primary importance.	• Reliable, low-cost, sustainable and scalable sensor networks (R1) • Next Generation IoT data processing architectures (R2) • Real time decision making for IoT (R3) • Autonomous IoT solutions (R4) • Future proof trust and security (R5) • Human in the loop IoT (R6) IoT & Data Semi-automated Interoperability (R8): as increasing automation in the interoperability will be key to increase IoT adoption.
Media	**Challenges**: The wide adoption of sensors in media sector demands for reducing costs of deployment. Beyond that the media sector is human / consumer centric, as such it poses a number of ethics, privacy, trust and security questions. **Value-added:** a better evolution of IoT technologies in the media field, especially within respect their interaction with the human factors, can revolutionize the media sector.	• Reliable, low-cost, sustainable and scalable sensor networks (R1) • Human in the loop IoT (R6) • IoT, Citizens, Privacy & Ethics (R9)
Insurance	**Value-added:** IoT adoption in the insurance industry, may lead to new models of risk assessment (including a user's credit & claims history, and the size and type of property owned etc.). **Challenges:** This poses a number of ethics, privacy, trust and security questions on IoT solutions	• Real time decision making for IoT (R3) • Human in the loop IoT (R6) IoT, Citizens, Privacy & Ethics (R9)
Transportation	**Challenges:** Mobility is a sector that can benefit enormously from IoT. Related deployment costs are still too high for real time decision making.	• Reliable, low-cost, sustainable and scalable sensor networks (R1) • Next Generation IoT data processing architectures (R2) • Real time decision making for IoT (R3)

Smart cities	**Value-added:** Smart Cities are more and more working toward the co-creation with citizens and businesses, by combining public sensors data and private ones. Cities, as shown by initiatives such as OASC, give primary importance to harmonised data models. **Challenges:** This demands for tackling privacy and ethics issues, on the other this requires that IoT system takes more into consideration human-based interactions, but still it is unclear how it is possible to incentivize data sharing. Moreover, large deployment for certain scenarios (e.g. public transport tracking) have still prohibitive costs.	• Reliable, low-cost, sustainable and scalable sensor networks (R1) • Real time decision making for IoT (R3) • Human in the loop IoT (R6) • IoT Data Sharing and Monetization enabling models and technologies (R7) • IoT, Citizens, Privacy & Ethics (R9)

Figure 27. Application domain specific challenges in relation to IoT

10. LOOKING AHEAD: CONCLUSION AND RECOMMENDATIONS

As highlighted by the economical, societal and research challenges discussed in Section 9.1 and 9.2, the Next Generation of IoT technologies will build on advancements in other scientific and technological areas (AI, Cloud, 5G/beyond 5G, Big Data /Data Analytics, etc.) and will require a multidisciplinary approach taking into consideration law, ethics, biology, sociology and psychology among others. In line with these outcomes, we consider as a key **initiative, the establishment of a transversal partnership among Cloud, IoT and Big Data stakeholders, both private and public, within Horizon Europe**. To ensure its relevance in the everyday life of European citizens and businesses, the initiative **should adopt a multidisciplinary approach, linking technology outcomes to research findings in law, ethics, biology, sociology and psychology regarding the adoption of IoT, Cloud and AI.** Such a partnership should focus on the development and piloting of open solutions combining the latest innovations in the smart connectivity arena with the ones in data processing and service infrastructure to deliver an infrastructure designed to meet the challenges of the Next Generation IoT. Such an initiative should also have a key role to **act as link and 'technology transfer' between the outcomes of the research and innovation initiatives within Horizon Europe and the implementation and deployment activities that form part of the Digital Europe Programme**.

Taking into consideration the different roles of Horizon Europe (focused on research and innovation) and Digital Europe (focused on the deployment of innovative digital technologies), we discuss below a set of recommendations for the two programmes based on priorities identified so far and discussed in Section 9.1 and 9.2,

10.1. Recommendations for the Horizon Europe programme

- Sustain activities around data value in the relevant work programmes, **increasing focus on IoT generated data** (R9, E3 & E8) (IA) **and on novel solutions for data processing** using IoT as a primary data source (R2) (RIA).
- Foster research in the Future Network area that will ensure the development of **reliable, low-cost, sustainable and scalable IoT networks** (R1 & E2) (RIA).
- Focus on the transition from data management to insight generation from data and on the increase of automation to reduce the cost of the management of complex IoT platforms and networks (R6 & R7) (IA).
- Leverage the advancements in Artificial Intelligence and Ledgers and other technologies to evolve IoT platforms beyond today's limitations (R2, R6 & R7) (RIA & IA).
- Prioritize the research on **machine-human** interaction in the IoT arena **following a multidisciplinary approach** (R8) (RIA).
- Support the establishment of large IoT trials in new domains beyond the ones covered today by IoT LSP (IA).
- Develop security-by-design and privacy-by-design IoT architectures and technologies (R3, R5) (RIA)
- Develop IoT miniaturisation, energy harvesting and pervasiveness (R7) (RIA)

10.2. Recommendations for the Digital Europe programme

- Support initiatives aimed at **increasing trust in IoT adoption through cybersecurity and privacy-by-design (GDPR compliance), as well as those seeking a better understanding of ethics and privacy** implications (R3, R5, E5, E6, & E8).
- Dedicate efforts to **support the creation of missing digital skills to support the large adoption of IoT within SMEs**, while supporting SMEs and startups in the development of innovative technologies (E1 & E4)
- Support the creation of a **set of open and royalty-free-to-use trustable classification and prediction algorithms covering key sectors of the European economy** (R6, E4 & E5)
- **Facilitate access to large computational facilities needed to harness the complexity of analysing terabytes** (or petabytes) of IoT generated data and ensure sovereignty (R6, R8, E1, E4 & E12).
- Sustain the **development of cross-domain harmonised data models**, following the path established by OASC, to **increase IoT application interoperability and replicability** especially in the public sector across Europe (R6, R8, & E7).
- **Transfer the experience matured by running LSP** in the sectors of Smart Cities, Smart Agriculture and Smart Healthcare to a wider set of actors **through Innovation Procurement** (E9) and similar actions.
- **Develop secure and highly scalable IoT network architecture, addressing schemes, and services** (R1, R2, R3, & R4) leveraging on global networking technologies such as IPv6 and 5G.
- **Contribute to global standardisation and interoperability of IoT** (R1, R4, & R9).
- **Leverage the potential of IoT for sustainable development**, in line with the UN Sustainable Development Goals (SDGs) (R8).
- **Contribute to the technological independence and autonomy of Europe in terms of IoT critical infrastructures and services** (R3, R5, & R7).

ANNEX II

IoT supporting COVID-19 prevention, diagnosis and treatment

Desk Review, NGIoT, 3 August 2020

With around 15 million confirmed cases of COVID-19 worldwide, measures to control the epidemic in various regions have leveraged IoT to manage patients, identify and isolate those infected and prevent transmission. While some European countries and New Zealand have virtually stopped COVID-19 from spreading in their territories, other regions are far from that milestone. On 2 April, 2020 the World Health Organization hosted a high-level meeting between technology and health experts, signalling the urgent need for digital solutions to help tackle this global threat.

Cecilia Bonefeld-Dahl, Director General of DIGITALEUROPE, has highlighted the need to increase spending on infrastructure for on-line access, 5G rollout and to accelerate the implementation of a common European data space for health. Data essential for tracking and fighting diseases should be shared between the public sector, researchers and private companies while maintaining strong security and data protection safeguards, she urged. (Parliament Magazine EU). These actions are among those highlighted as innovation drivers by NGIoT's IoT scoping paper.

Fig. 1: The digital sector's support against Coronavirus, source DIGITALEUROPE

CONTACT TRACING

The scale of COVID-19 infections has outstripped governments' capacities to conduct manual contact tracing. Existing contact tracing practices are resource intensive, slow and often subject to recall bias. Therefore, contact tracing apps harnessing Bluetooth technology adopted by governments is one of the main ways IoT can support disease control.

People infected with COVID-19 are possibly infectious before they become symptomatic, with one estimate being that 50 percent of all new COVID-19 infections being transmitted from someone who is either pre-symptomatic or asymptomatic, (Science). Therefore, contact tracing is moving beyond tracking people with symptoms of the virus, to tracking health in general. UK researchers have developed a symptom tracking app that prompts users each day to record any symptoms and general wellbeing, the COVID-19 Symptom Tracker App 2020 (Mass General Cancer Center). Data from wearable smart devices, such as fitness apps could provide diagnostic support by detecting physiological changes (ABC News). The German Health Authority has already launched an application to collect wearable data voluntarily from citizens (The Star). Data could be incorporated into machine learning algorithms to try and provide diagnostic and surveillance support to health agencies.

Applications should enable users to control their data, collect only relevant data and have clear procedures for use by health authorities. Fear of loss of data security affects uptake. To maximise the uptake of case reporting there is a need for coordination and leadership. In Singapore, reports suggest around only 16 percent uptake of their contact tracing app (Radio NZ).

At the initiative of the European Commission and in line with the Toolbox for Tracing Apps published in April 2020, representatives of the NGI community set up a technical review facility that provides independent security and privacy analysis of COVID-19 related technology. The Emergency Tech Review Facility is a collaborative, community-focussed effort to quickly and transparently analyse COVID-19 tech solutions to improve trust in technology which could lead to wider uptake.

The Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) makes it possible to interrupt new chains of SARS-CoV-2 transmission rapidly and effectively by informing potentially exposed people. The non-governmental organisation (NGO) provides standards, technology, and services to countries and developers, with an emphasis on preserving privacy. PEPP-PT builds on tested, fully implemented proximity measurement and scalable backend service, to enable tracing of infection chains across national borders.

The Australian federal government has sought to allay privacy concerns with its contact tracing app by proposing a jail term of up to five years for those that use COVIDSafe data for any purpose other than contact tracing. Australia's peak Internet of Things (IoT) industry body, IoT Alliance Australia (IoTAA), and Telstra, Optus and others have funded a COVID-19 discussion hub that examines the industry's response to the crisis. (IoT Hub).

AI, BIG DATA & SURVEILLANCE

Access to public information has led to the creation of national and regional dashboards that are continuously monitoring the virus, requiring the development of dashboards using Big Data and AI.

The European Commission will invest in the use of Artificial Intelligence to speed up the diagnosis of COVID-19 and improve future treatment of patients. A software developed to assist the work of medical staff by analysing images of pulmonary infections is introduced in 10 hospitals across Europe. The AI tool will allow the diagnosis of COVID-19 in less than one minute. The algorithm uses the images collected by a computerised tomography (CT) scanner (usually an integral part of a hospitals' infrastructure) to detect COVID-19 suspicious cases (European Commission).

An EU-funded consortium is using an EU-backed supercomputing platform, one of the world's most powerful, to check the potential impact of known molecules against the genomic structure of coronavirus. Exscalate4CoV has announced that an already registered generic drug used to treat osteoporosis, Raloxifene, could be an effective treatment for COVID-19 positive patients with mild or asymptomatic infection (European Commission).

China has created a massive surveillance system to fight the virus and is using Big Data and Machine Learning to analyse data. The Chinese government is gathering people's smartphone location data, body temperatures, travel history and other details in a centralised database. Thousands of facial recognition-powered CCTV cameras have also been installed at almost every quarantine center and only those who have been assigned the green colour code can drive on the roads. WeChat, the popular instant messaging app that also has a digital wallet, is being used to collect data. (Geospatial World). Chinese AI companies like SenseTime and Hanwang Technology have claimed to come up with a special facial recognition technology that can accurately recognize people even if they are masked. CCTV cameras have also been installed at most locations to ensure that those who are quarantined do not leave their homes. (Geospatial World). Baidu has also made tools to screen large populations and an AI-powered infrared system that can detect change in a person's body temperature. It was being used in Beijing's Qinghe Railway Station to identify passengers who were potentially infected. The system can examine up to 200 people in one minute without disrupting passenger flow. (Geospatial World).

To mitigate the epidemic and accurately scan people diagnosed with the virus, countries across the globe are tracking smartphone data. For instance, in Australia, it has become mandatory for all mobile connectivity companies to save at least two years of data of every person, including data regarding his whereabouts, or simply location data. This data would be critical in examining the travel history of the person who has tested positive. It would also become easier to spot any phone that has been in close range of the infected person's phone in the past few months. The owners of those phones can then be screened, irrespective of whether they have developed symptoms. (Geospatial World).

US, Singapore, Poland, Israel and South Korea are some of the other countries that are using smartphone tracking. It is believed that the British government is discussing the possibility of location data tracking with British Telecom, the country's biggest operator. A Washington Post report says that the White House is in talks with tech giants like Google and Facebook to effectively track user location data and gain insights from it. Further, reports suggest that most global telecom

companies are planning to develop a comprehensive framework that will enable sharing of data on an unparalleled scale. (Geospatial World).

Bio-surveillance could emerge as normal, recording the pulse rate, blood pressure and other biological parameters that drastically change when people feel happy, sad and angry. If a government knows what makes a particular person cheerful or gloomy, it can very easily devise strategies for manipulation. (Geospatial World).

The Chinese government joined hands with tech giants Alibaba and Tencent to develop a color-coded health rating system that is tracking millions of people daily. The smartphone app was first deployed in Hangzhou in collaboration with from Alibaba. It assigns three colours to people — green, yellow and red — on the basis of their travel and medical histories. In the industrial hub of Shenzhen, a similar software was created by Tencent.

Whether a person should be quarantined or allowed in public spaces was decided based on the colour code. Citizens had to log into the app using pay wallet services like Alibaba's Alipay, Ant's wallet, etc. Only those people who were assigned a green colour code could be allowed in public spheres after using the designated QR code at metro stations, offices and other public places. There were checkpoints at most public places where the code and a person's body temperature was checked. More than 200 Chinese cities were using this system. (Geospatial World).

BORDER CONTROL

Hong Kong and South Korea use GPS data for quarantining procedures. In Hong Kong, incoming passengers are provided with wristbands that link to a GPS-enabled smartphone to enforce self-isolation rules source (Straights Times).

In New Zealand, incoming passengers' address information is already routinely collected (The Conversation). A digital app that uses GPS data may enable passengers to update their self-isolation plan online to expedite screening procedures, help monitoring and enforcement of self-isolation rules and provide support to visitors during their self-isolation period. (Public Health Expert).

MEDICAL IoT

At present, there are no effective antiviral drugs against COVID-19, therefore case identification and monitoring are vital. The application of the IoT to medicine is referred to as the medical IoT (MIoT) which aims to establish a decision-oriented big data analysis model supported by information technology such as communication, electronics, biology, and medicine.

The current diagnosis of COVID-19 is mainly dependent on viral nucleic acid testing (NAT). The accuracy of current nucleic acid testing is approximately 30–50 percent (Clinical eHealth[1]). NATs differ from other tests in that they detect genetic materials (RNA or DNA) rather than antigens or antibodies. Detection of genetic materials allows an early diagnosis of a disease because the detection of antigens and/or antibodies requires time for them to start appearing in the bloodstream.

Computed Tomography' (CT) can precede the detection of nucleic acid tests in some patients. CT refers to a computerized x-ray imaging procedure in which a narrow beam of x-rays is aimed at a patient and quickly rotated around the body, producing signals that are processed by the machine's computer to generate cross-sectional images of the body (Wikipedia).

The aforementioned software developed to assist the work of medical staff by analysing images of pulmonary infections (European Commission); as well as the EU-funded Exscalate4CoV consortium, which is using an EU-backed supercomputing platform, to identify a treatment for COVID-19 (European Commission) demonstrate development of MIoT in Europe.

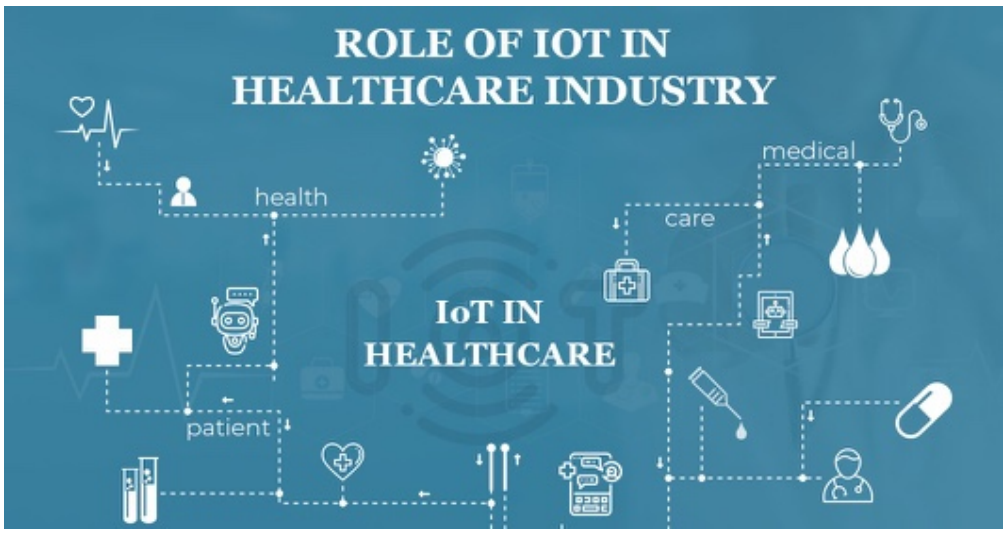


Figure 2, IoT in Healthcare, source: IoT Magazine

With the help of data analytics and predictive models, medical professionals can understand more about diseases. Baidu, the Chinese Internet giant, has made its Lineatrfold algorithm available to teams that are fighting the outbreak, according to the MIT Technology Review. Unlike Ebola, HIV and Influenza, COVID-19 has only a single strand RNA, so it is able to rapidly mutate. The algorithm is a lot faster than other algorithms that help predict the structure of a virus. (Geospatial World).

In China, Alibaba has developed a Cloud-based Coronavirus diagnosis tool that the company claims is more than 96 percent accurate and takes less than 20 seconds to work. The tool uses AI to detect traces of the virus. Alibaba says that it has been used on more than 5,000 patients throughout China. (Geospatial World).

[1] Chinese experts' consensus on the Internet of Things-aided diagnosis and treatment of coronavirus disease 2019 (COVID-19) Author: Li Bai,Dawei Yang,Xun Wang,Lin Tong,Xiaodan Zhu,Nanshan Zhong,Chunxue Bai,Charles A. Powell,Rongchang Chen,Jian Zhou,Yuanlin Song,Xin Zhou,Huili Zhu,Baohui Han,Qiang Li,Guochao Shi,Shengqing Li,Changhui Wang,Zhongmin Qiu,Yong Zhang,Yu Xu,Jie Liu et al., Publication: Clinical eHealth, Publisher: Elsevier, Date: 2020 https://www.sciencedirect.com/science/article/pii/S2588914120300046

MIoT is the basis of China's "COVID-19 Intelligent Diagnosis and Treatment Assistant Program (nCapp)". Considering the different levels of diagnosis and treatment among doctors in different regions and hospitals, some cases are still missed or misdiagnosed, especially when the nucleic acid test has a negative result (Clinical eHealth[2]).

The IoT nCapp cloud medical system platform contains the basic functions of IoT and has a core graphics processing unit (GPU). Cloud computing systems connected to existing electronic medical records, image archiving, and picture archiving and communication can better assist in deep mining and intelligent diagnosis. The functions of IoT are considered to be beneficial time assistance, supervision, and control of medical quality; as well as online monitoring, location tracking, alarm linkage, and follow-up scheduling; and finally systems management, remote maintenance, command management, and statistical decision-making functions, which can expand the massive information mining of COVID-19. It can also assist in asking questions; registering patients' details; coordinating with patients, community doctors, and experts; and providing safe diagnosis treatment programs and two-way referrals.

The three-linkage IoT cloud plus terminal nCapp COVID-19 diagnosis and treatment system uses 5G technology to meet the overall system's network requirements for network liquidity, efficiency, high load, and high capacity platform. Based on the WeChat, an nCapp smartphone app can coordinate the division of labour in the diagnosis and treatment of COVID-19 in one-, two-, and three-tier hospitals and perform three-level linkage among experts, primary doctors and service providers. nCapp can also be used by visualization techniques. The data visualization method of the system, with the cloud plus augmented reality, enable doctors and patients to communicate in an augmented reality way, to reduce cross infection.

China launched the "5G + Cloud + AI" pneumonia intelligent auxiliary analysis system that improves the accuracy of virus detection and shortens the time of CT scanning. Early data shows that the system can control the reading time within 1 minute through the AI algorithm, with detection accuracy greater than 90 percent which represents a significant improvement in the efficiency of epidemic diagnosis and treatment (China Telecom Americas).

HOME CARE & TELEHEALTH

In Japan, IoT and AI assist nursing care during the pandemic amid a labour shortage. Sensors monitor the lifestyle habits of the elderly while AI-initiated phone calls check on seniors daily, allowing caregivers to look after them remotely. The person's home is equipped with sensors installed in the bathroom, bedroom and refrigerator, as well as attached to doors, providing the care manager with data via the internet on how frequently he uses the bathroom, how long he sleeps and whether he has eaten. (Kyodo News)

[2] Chinese experts' consensus on the Internet of Things-aided diagnosis and treatment of coronavirus disease 2019 (COVID-19) Author: Li Bai,Dawei Yang,Xun Wang,Lin Tong,Xiaodan Zhu,Nanshan Zhong,Chunxue Bai,Charles A. Powell,Rongchang Chen,Jian Zhou,Yuanlin Song,Xin Zhou,Huili Zhu,Baohui Han,Qiang Li,Guochao Shi,Shengqing Li,Changhui Wang,Zhongmin Qiu,Yong Zhang,Yu Xu,Jie Liu et al., Publication: Clinical eHealth, Publisher: Elsevier, Date: 2020 https://www.sciencedirect.com/science/article/pii/S2588914120300046

In the U.S., the Mayo Clinic is reportedly in talks with "makers of remote monitoring tools about ways to keep closer tabs on patients with COVID-19 who don't require intensive care." Similarly, to keep non-COVID patients healthy at home that other IoT devices measure "health metrics like temperature, blood pressure and blood sugar several times a day, and the results are automatically stored on the cloud, from which doctors get alerts if the readings are abnormal." (TIME)

Beyond collecting individual health stats, IoT devices are tracking community-level data, which in turn is used to better understand the evolution of the virus. Retail drugstores track inventory and sales of non-prescription fever reducers, for example, and any trends in those data might serve as an early, albeit crude, harbinger of growing spread of disease in a community (TIME).

The "U.S. health weather map" powered by Kinsa Insights provides a visualization of aggregated data on fevers and flu-like illnesses. Healthcare providers can then use the maps to identify areas where there are spikes in illness and gauge whether measures are successfully helping to slow the spread of COVID-19 in other areas.

The pace of IoT innovation in telehealth to fight a pandemic—that fundamentally requires a reduction in person-to-person contact—means that companies are launching innovation *before* security strategies…sometimes even before the technology is ready. History has shown that exactly these types of circumstances are when hackers are more likely to strike. (Security Boulevard)

ROBOTICS & DRONES

In order to scale critical ICU nursing resources during the outbreak in Wuhan, China, a field hospital was staffed primarily with IoT robots to clean, disinfect, deliver medicines and take patients' temperatures in the hospital. Hospital administrators indicated that the robots both better scaled nursing resources for critical care as well as lessened the transmission of the virus to hospital staff (NBC).

Robots in China are preparing meals at hospitals, providing waiter service in restaurants, spraying disinfectants, vending rice and dispensing hand sanitizers. In many hospitals, robots were also performing diagnoses and conducting thermal imaging. Shenzhen-based company Multicopter is using robots to transport medical samples. (Geospatial World). A hospital in Wuhan, the epicenter of the outbreak, was being staffed entirely by robots. Wuchang Hospital, China Mobile and Cloud Minds, a manufacturer of Cloud-based robotics systems, came together for this project aimed at making the hospital facility completely smart and digital. Most of the devices in the hospital are IoT enabled and services are carried out by robots. The initial screening of the patients is done by 5G-enabled thermometers that send instant updates. Also, there are rings and bracelets that are connected to the CloudMinds AI platform so that it can monitor all changes in the body. (Geospatial World).

As per a Reuters report, a small robot called Little Peanut was delivering food to passengers on a flight from Singapore to Hangzhou, China who were being held under quarantine in a hotel. (Geospatial World). CloudMinds alone has deployed 100 robots in the country's hospitals. A few

modified robots like Cloud Ginger (aka XR-1) and the Smart Transportation Robot carry food and medicine to patients from healthcare providers without any human contact. (Geospatial World). In some of the severely affected areas, where humans were at a risk of catching the virus, drones came to the rescue. Drones were transporting both medical equipment and patient samples, saving time and enhancing the speed of deliveries, while preventing contamination of medical samples. (Geospatial World).

Drones were also flying with QR code placards that could be scanned to register health information. Drones powered with facial recognition were also being used to broadcast warnings to the citizens to not step out of their homes and chide them for not wearing face masks. Antwork, a group company of Japanese dronemaker Terra Drone, carried medical samples and other essential materials in Xinchang when the city was grappling with the virus. (Geospatial World).

GLOBAL NAVIGATION SYSTEM OF SYSTEMS

Global Positioning technologies play a crucial role in epidemics. In China, BeiDou, the country's own GNSS constellation, helped track patients and affected places. With the help of reliable data and precise mapping and imagery, China could build thousands of new makeshift hospitals across the country (Geospatial World). According to reports, the Chinese government was able to hasten the construction of two new hospitals in Wuhan mainly due to BeiDou.

In Ruichang, Jiangxi province, the police forces are using BeiDou-enabled drones for monitoring congested public areas. The Chinese Ministry of Transportation was able to swiftly send emergency messages to over 6 million connected vehicles using BeiDou. The Chinese e-commerce giant JD also delivered medical equipment in remote hospital areas in Wuhan with the help of robots based on BeiDou (Geospatial World).

While dozens of makeshift hospitals were being constructed their progress was continuously being monitored using GaoFen, a constellation of high-resolution Earth observation satellites. Zhuhai-1 hyperspectral imaging satellite and ESA's Sentinel-1 also helped in non-stop monitoring of hospital construction. The Wuhan University actively collected and analysed multiple data sources and identified which site would be best suitable for the hospital (Geospatial World).

TFSTAR, a second generation AI satellite designed by the Satellite Technology Research Center of University of Electronic Science and Technology of China (UESTC) and ADA-Space, is capable of powerful analytics and processing, which enables it to sift through the data. By combining TFSTAR's data processing capability with geocoding, a health visualization of COVID-19 was created on which people could see the geographical reach of the virus and could find out the distance between them and active infection (Geospatial World).

AUTONOMOUS VEHICLES

At a time of severe crunch of healthcare professionals and the risk of people-to-people contact, autonomous vehicles are proving to be useful delivering medicines and food items. Apollo, which is Baidu's autonomous vehicle platform, has joined hands with self-driving startup Neolix to deliver supplies and food to a big hospital in Beijing. Baidu Apollo has also made its micro-car kits and autonomous driving Cloud services available for free to companies fighting the virus. Idriverplus, a Chinese self-driving company that operates electric street cleaning vehicles, is also a part of the mission. The company's flagship vehicles are being used to disinfect hospitals. (Geospatial World).

One study looking at IoT applications to fight against the COVID-19 pandemic searched the databases of Google Scholar, PubMed, SCOPUS and ResearchGate using the keywords "Internet of Things" or "IoT" and "COVID-19". Further inputs are also taken from blogs and relevant reports. Results were found to support the view that IoT implementation impacts on reducing healthcare cost and improve treatment outcome of the infected patient. IoT is helpful for an infected patient of COVID-19 to identify symptoms and provides better treatment rapidly. It is useful for patient, physician, surgeon and hospital management system. (Elsevier Public Health Emergency Collection)

Beep, an autonomous shuttle service provider, said in early April that it was partnering with the Jacksonville Transportation Authority and shuttle maker Navya to transport COVID-19 tests at Mayo Clinic in Florida. (Reuters)

CONCLUSION

In Europe, IoT is part of the solution to COVID-19 prevention, diagnosis and treatment efforts. In terms of medical IoT, software developed to assist the work of medical staff by analysing images of pulmonary infections as well as use an EU-backed supercomputing platform, to identify a treatment for COVID-19 are prominent examples. The EC's COVID-19 technical review facility attempts to strike the balance between disease control and the protection and privacy of citizens' data.

Globally, the application of innovative IoT in smart health and care for COVID-19 disease transmission, monitoring, diagnosis and treatment is in evidence in a wide range of activities. Tech solutions were quickly identified and adapted for healthcare and both government agencies and medical authorities are relying on technology linked to IoT for contact tracing, Medical IoT, and Homecare and Telehealth. Prevention measures are in place harnessing big data and surveillance as well as border controls. Robotics, drones, GNSS and autonomous vehicles are increasingly being adopted to assist medical procedures while minimising the spread of the virus. ESA's Sentinel-1 also helped in non-stop monitoring of hospital construction in China.

Certain innovation drivers identified by NGIoT's IoT scoping paper (Edge computing, 5G, AI and analytics) are pre-requisites to the technologies listed above; while others (AR and tactile Internet, digital twins, distributing ledgers and nano electronics) are not yet in evidence in the fight against COVID-19, according to this current desk review, concluded 3 August, 2020.