# BUILDING A ROADMAP FOR THE NEXT GENERATION INTERNET OF THINGS

## RESEARCH, INNOVATION AND IMPLEMENTATION 2021-2027

## SCOPING PAPER

NEXT GENERATION INTERNET OF THINGS

ngiot.eu

**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



| | |
|---|---|
| Lead Editors (in alphabetical order) | Martin Brynskov (Aarhus University), Federico Michele Facca (Martel Innovate), Gabriela Hrasko (Archimede Solutions) |
| Contributors (in alphabetical order) | Anna Brékine (Mandat International), Martin Brynskov (Aarhus University), Monique Calisti (Martel Innovate), Benoît Dalbert (Aarhus University), Olivia Doell (Archimede Solutions), Federico Michele Facca (Martel Innovate), Adriënne Heijnen (Aarhus University), Gabriela Hrasko (Archimede Solutions), Ana Maria Pacheco Huamani (Archimede Solutions), Kseniia Kalugina (Aarhus University), Lamprini Kolovou (Martel Innovate), Sébastien Ziegler (Mandat International) |
| Version | 1.0 |
| Date | 11th September 2019 |



## Feedbacks

NGIoT consortium welcomes feedbacks on the Scoping Paper.
Use the QR Code (or the following link: https://forms.gle/cBzgnaZo5TdeMWoB6) on the side to access a feedback form.
The feedbacks will be used for the roadmap activities of NGIoT.

## Important Notice: Working Document

This scoping paper is intended to support the European Commission in setting priorities for Horizon Europe (HEU), the framework programme for research and innovation, and the Digital Europe Programme (DEP) for the implementation and deployment of digital technologies. It is a working document not formally endorsed by the European Commission, and its content does not in any way prejudge the final decision of the European Commission on the aforementioned programmes.

This scoping paper is an outcome of the Next Generation Internet of Things (NGIoT) project, a Coordination and Support Action that has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement no 825082.

# Executive Summary

The objective of this scoping paper is to analyse Internet of Things (IoT) research, innovation and implementation challenges and present a set of recommendations for future IoT-focused investments to support the European Commission (EC) in the definition of the Horizon Europe and Digital Europe programmes for 2021-2027, as well as guide other initiatives in EU member states and among the IoT landscape in general, in Europe and beyond. The scoping paper is a preliminary step towards a roadmap for IoT research, innovation and implementation that is a planned output of the Next Generation Internet of Things (NGIoT) project[1]. The roadmap will provide the European Commission and the IoT community with valuable insights on research, innovation and implementation priorities to secure the development of the Next Generation Internet of Things (NGIoT) technologies that shall be secure, safe, trusted and human-centric. This will help shape the future of our society, economy and planet. Concretely, it will lead to the support of a fair and climate-neutral data economy, an increase in digital capacity and skills in the EU, maximising the economic and societal benefits as a consequence of better trusted and secure technologies, building a world-leading connectivity infrastructure which will boost the development of the IoT European community and ecosystem, situated in a complex geopolitical situation.

Increasing the adoption of IoT technologies is a delicate matter. On the one hand, IoT has the potential to bring huge opportunities. On the other hand, it carries several associated risks and challenges. The NGIoT scoping paper highlights potential actions to be taken to ensure that Europe will play a leading role in a human-centric digital transformation, delivering benefits to all citizens on all levels, and in both the private and public sectors. By studying and assessing priorities and challenges, while consulting experts and supporting communication and community building at the service of European IoT, NGIoT aims to provide recommendations to the for future investments to the EC as well as member states, regulators and other stakeholders on both the demand- and supply-side of the market. By building on major EU-driven initiatives around IoT, such as the IoT European Large-Scale Pilots (IoT LSP), Alliance for Internet of Things Alliance (AIOTI), European Platforms Initiative (EPI-IoT), Next Generation Internet (NGI), 5G Public Private Partnership (5G PPP), Big Data Value Association (BDVA), FIWARE, European Cybersecurity PPP and the European Technology Platform on Smart Systems Integration Strategic Research Agenda (EPoSS SRA), and linked to existing programmes such as the Connecting Europe Facility (CEF) and the European Interoperability Framework (EIF), the ambition is also to provide an insightful and comprehensive view of the IoT evolution.

This scoping paper is based on the outcomes of the online IoT Research and Development Survey[2], on the analysis of several IoT research and strategy reports, on information gathered at IoT-focused conferences, as well as on input gathered from selected experts and key stakeholders. The NGIOT online survey was conducted from March to June 2019 to get a more in-depth insight on the IoT community view. The survey gathered answers from 284 participants from 29 countries

[1] Next Generation Internet of Things (NGIoT) is an H2020 Coordination and Support Action (CSA): http://ngiot.eu

[2] The IoT Research and Development Survey was developed to collect IoT stakeholders' input under the umbrella of the NGIoT project.

(mostly European) representing mostly companies (45 percent, of which 28 percent are SMEs and 17 percent industry) and research institutions (36 percent). The identified priority topics for the NGIOT include **security/cybersecurity**, **privacy, safety** (i.e. data protection) as well as **interoperability**. The most relevant application domains, according to the outcomes of the survey, are **smart cities & communities, health** and **mobility** followed by **industry, energy, environment/climate** and **agriculture/agri-food**.

IoT has and will have a significant impact on the worldwide economy, both at macro- and micro-economic level. Europe is reported to account for 23 percent of the global IoT market and ranks second after the USA, but in a highly volatile landscape. An economy with higher investment in IoT is likely to experience an increase in trade surplus and a stronger impact on the governance around global digital platforms. The implementation of IoT technologies brings transformation across and between many, if not all, domains. On the job market, it is facilitating the creation of new (types of) jobs. The need for experts in IT/ICT, big data scientists, software engineers and several other computing and networking related jobs is expected to increase, and other less-skilled job categories will likely decrease. The new types of jobs and ways of working will bring both societal and organisational challenges. Using the instrument of public procurement to drive innovation and to ensure sensibility to societal priorities is a key strategy. The extended availability of measurements, dynamic data collection and mathematical algorithms will enable well-informed decision-making and optimisation of processes leading to an increased ability to impact positively on a triple baseline of people, planet and profit.

In this scoping paper, we focus on **seven key application domains from the economic perspective, which are**: Energy Management, Manufacturing, Transportation, Smart Cities & Communities, Healthcare, Smart Food & Farming and Retail, including three additional emerging domains: Media, Insurance and Safety & Defence. Moreover, **twelve key challenges are explored from an economic and policy perspective**: Support for SMEs and start-ups (E1), Accurate Economic Parameters Estimates (E2), Data and Information as Critical Assets (E3), Increase of Digital Skills and Competencies (E4), Build Trust (E5), Identification of the Key Regulatory and Legal Issues (E6), Interoperability and Replicability (E7), Security and Reliability by Design (E8), Innovation Procurement (E9), Sustainability (E10), Cohesion (E11), and Sovereignty (E12).

At a **technological/scientific level**, IoT progress is heavily interconnected with advances in several fields, including **Edge Computing, 5G, Artificial Intelligence and Analytics, Augmented Reality and Tactile Internet, Digital Twin** and **Distributed Ledgers**. In relation to that, from a more specific R&D perspective, the scoping paper reports on five fundamental challenges: Reliable, low-cost, sustainable and scalable sensor networks (R1), Next Generation IoT data processing architectures (R2), Future proof trust and security (R3), IoT, processes & data semi-automated interoperability (R4), IoT, citizens, privacy & ethics (R5). As emerging challenges, we identified: Real Time Decision Making for IoT (R6), Autonomous IoT solutions (R7), Human-in-the-loop IoT (R8), IoT data sharing and monetisation enabling models and technologies (R9).

Overall, based on the work conducted so far, the scoping paper highlights the need for **the establishment of a transversal partnership among European Cloud, IoT and Big Data stakeholders, both private and public sector, within Horizon Europe** and a set of recommendations for future IoT-focused investments in the Horizon Europe and Digital Europe Programmes.

**Recommendations for the Horizon Europe programme**

- **Increase focus on privacy-by-design IoT-generated data** (R9, E3 & E8) (IA) **and on novel solutions for data processing** using IoT as 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 management of complex IoT platform** 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 multi-disciplinary approach** (R8) (RIA)
- **Support the establishment of large IoT trials in new domains, including cross-domain**, beyond the ones covered by IoT LSP (IA)
- **Develop security-by-design and privacy-by-design IoT architectures and technologies** (R3, R5) (RIA)
- Develop **IoT miniaturization, energy harvesting and pervasiveness** (R7), (RIA)

**Recommendations for the Digital Europe programme**

- Support initiatives aimed at **increasing trust in IoT adoption building on cybersecurity and privacy-by-design, as well as 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 Start-ups 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 and inclusive 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 minimal interoperability mechanisms (MIMs)** to **increase IoT application interoperability and replicability** especially in the public sector across Europe (R6, R8, & E7)
- **Transfer the experience matured within LSPs** in the sectors of Smart Cities & Communities, Smart Agriculture and Smart Healthcare to a wider set of actors **through Public Procurement, including 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 technological independence and autonomy of Europe in terms of IoT critical infrastructures and services** (R3, R5, & R7).

# Table of contents

# 1. INTRODUCTION

The Internet of Things (IoT) embraces a diversity of highly impactful application domains, from farming to industry and leisure. The European research and innovation community has played a leading role in pioneering and developing IoT technologies and solutions in various domains, including eHealth, connected vehicles, smart cities & communities, environmental monitoring and energy efficiency.

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.

## 1.1. Scope and objectives

This scoping 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 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.

The scoping paper is the first step towards developing a Research, Innovation and Implementation Roadmap for the Internet of Things in Europe for the period 2021-2027. The roadmap 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.).
- 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 develop 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 scoping paper has been organised to create and deliver meaningful insights and recommendations for public and private investments with a view to a more extended road map that will follow the scoping paper.

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 and workshops,
  - Feedback from the NGIoT Strategy Board,
  - 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 who received a first draft of the scoping paper at the beginning of June 2019 and provided feedback. Validation is still ongoing, as well as further information gathering, as the current version of the scoping paper is planned to be improved according to relevant feedback and integrated into the NGIoT roadmap.

- **Outreach Phase.** The scoping 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, that will lead to the shaping of an IoT research and innovation roadmap. 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.

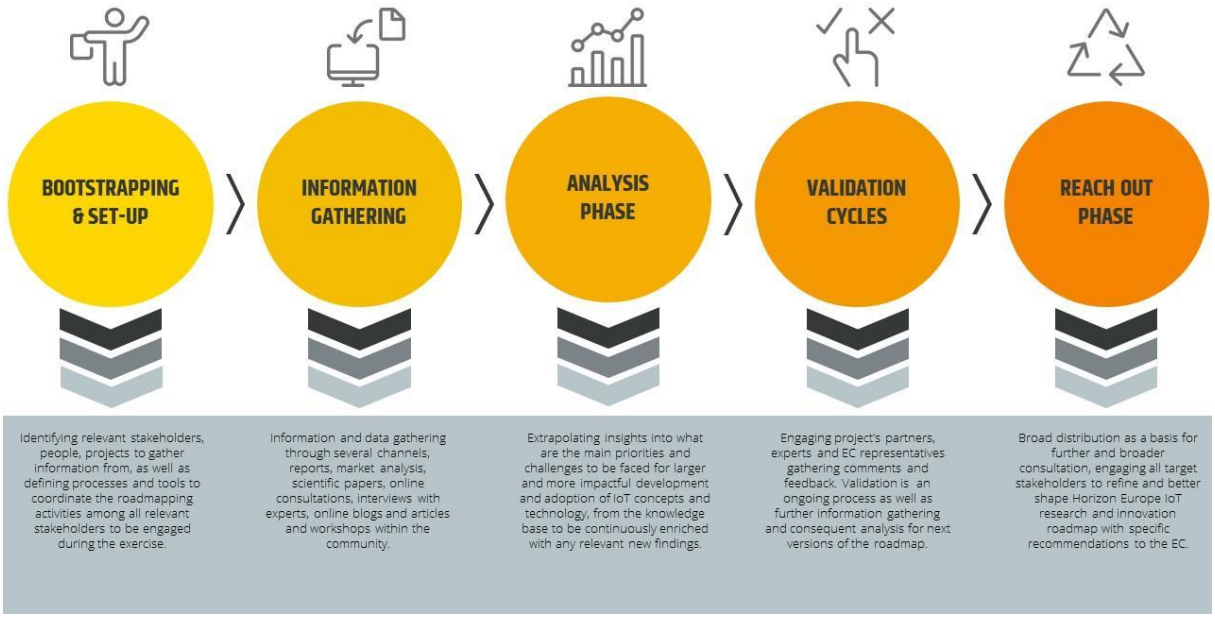


*Figure 1. Scoping Paper Methodology*

# 2. BACKGROUND INFORMATION

## 2.1. Context

The Internet has become an integral part of our daily life: the way people act, interact and present themselves to one another is heavily influenced by living and acting in a semi-virtual dimension. Yet, 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.'[3]

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[4].

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, 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[5].

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

[3] https://ngi.eu/wp-content/uploads/sites/48/2019/08/NGI_An-Internet-of-Humans.pdf
[4] https://nlnet.nl/NGI/reports/NGI-Study-ISBN-9789279864667.pdf
[5] https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-leit-ict_en.pdf

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 and coming roadmap should be seen in this light, supporting directly this ambition of the EC.

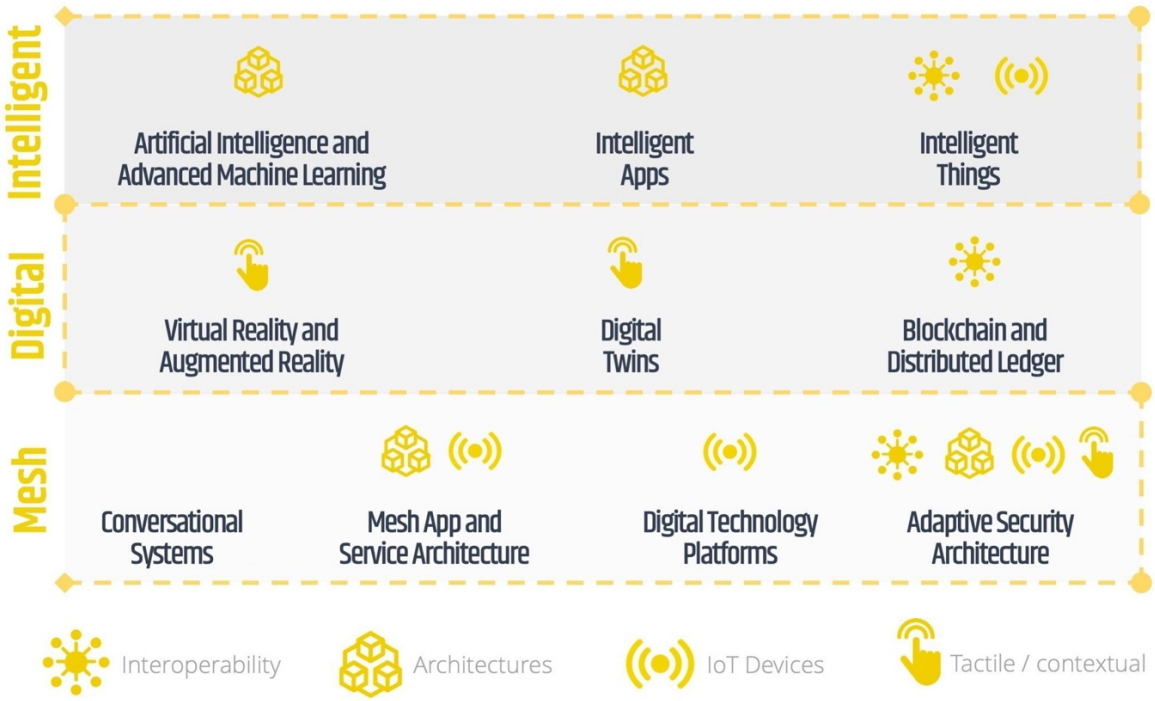


*Figure 2. European Research, Innovation and Implementation related to Internet of Things*

## 2.2. 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[6]. 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.

[6] 78% of responses came from EU countries, in particular, in order of importance: Spain, Greece, Belgium, Denmark, Germany, Italy and Sweden.

- 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.

# 3. BUILDING ON WHERE WE ARE TODAY

## 3.1. EU strategy from 2014 to 2020

In line with the Digital Single Market Strategy[7] and its pillar 'maximising the growth potential of digital economy', the European Commission launched the Digitising European Industry (DEI) initiative[8] 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'.[9] 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.

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[10] (AIOTI) to coordinate ongoing activities and build a consensus on how to unleash the full potential of IoT 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.'[11]

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[12] 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.'[13]

In 2016, the IoT-European Platforms Initiative[14] was formed to promote the idea of open and easily accessible platforms and to build a vibrant and sustainable IoT-ecosystem in Europe.

---

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0180&from=EN
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN
[10] https://aioti.eu/
[11] https://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-focus_en.pdf
[12] http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-leit-ict_en.pdf
[13] https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/dt_booklet.pdf
[14] https://iot-epi.eu/

In the same year, the IoT Large-Scale Pilots (LSPs) Programme[15] 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[16] 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 sovereignty in the Digital Age. As outlined in a recent Strategic Note[17], digital technologies and the global race for technological R&I leadership will play a pivotal role in ensuring Europe's strategic autonomy.

## 3.2. The European landscape

As reported in the **IoT LSP** Programme eBook[18], 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.

The **AIOTI** Strategy 2017-2021[19] 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.

---

[15] https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf
[16] https://ec.europa.eu/digital-single-market/en/research-innovation-iot
[17] https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf
[18] https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf
[19] https://aioti.eu/aioti-strategy-2017-2021/

Along the same line, the **Road2CPS** Technology and Application Roadmap[20], 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)[21] 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[22] 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**[23] 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[24] 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

[20] http://road2cps.eu/events/wp-content/uploads/2016/03/Road2CPS_D2_4_StrategyRoadmap-submission.pdf
[21] http://www.bdva.eu/SRIA
[22] https://www.fiware.org/community/fiware-mundus/
[23] https://www.networld2020.eu/wp-content/uploads/2018/11/networld2020-5gia-sria-version-2.0.pdf
[24] https://ecs-org.eu/documents/ecs-cppp-sria.pdf

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

The **EPoSS SRA**[25] adopts, presents and supports all the challenges, critical needs and statements shared by all previous initiatives, providing also a deep analysis on both the fields and the transversal topics around and with IoT in practice, including transport and mobility, health and well-being, manufacturing, energy and security, but also other technologies for smart systems, reliability and process management.

Finally, the report provided under the **NGI Initiative**[26] 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.

## 3.3. The international picture in IoT

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[27], 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'[28] 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'[29], 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.

[25] https://www.smart-systems-integration.org/system/files/document/2017%20EPoSS%20SRA_0.pdf
[26] https://www.ngi.eu/wp-content/uploads/sites/18/2019/02/HUB4NGI-D2-3-NGI-Guide-v3-v1.2.pdf
[27] https://www.us-ignite.org/program/smart-gigabit-communities/
[28] http://promexico.mx/documentos/mapas-de-ruta/industry-4.0-mexico.pdf
[29] https://www.nedo.go.jp/content/100865202.pdf

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[30], 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[31], 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[32], 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[33], 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[34]. 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[35] 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"[36] 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.

[30] https://www.smartnation.sg/
[31] https://www.smartnation.sg/what-is-smart-nation/initiatives/Strategic-National-Projects/smart-nation-sensor-platform
[32] https://www.a-star.edu.sg/Research/Research-Focus/Infocomms/IIOT
[33] https://www.mestecc.gov.my/web/wp-content/uploads/2017/02/IoT-Strategic-Roadmap-1.pdf
[34] http://smartcities.gov.in
[35] dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf
[36] http://www.nstf.org.za/wp-content/uploads/2017/04/National-ICT-Policy-White-Paper.pdf

# 4. ECONOMIC OPPORTUNITY FOR EUROPEAN RESEARCH AND INNOVATION

This section summarises the insights from various market analyses. It identifies and extracts the key IoT application domains from the economic perspective and the key economic and policy challenges. The implementation of IoT technologies is linked with significant economic opportunities, which should be exploited to bring back value to society and give an overall boost to European competitiveness at a global level.

## 4.1. IoT adoption in Europe vs the rest of the world

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[37]. These forecasts illustrate the expected rapid growth of IoT devices in comparison to the growth in the number of generally connected devices. 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[38]. 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)[39]. 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. The global IoT market shares by sub-sector are dominated by smart cities (26 percent), industrial IoT (24 percent), medical and healthcare (20 percent) and smart homes (16 percent). Other relevant sub-sectors include connected cars, energy management, wearables, smart utilities and others[40]. 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, asset tracking, remote monitoring, preventative maintenance, compliance monitoring, remote diagnostics, etc.

Based on the analysis of the IoT market, most of the projects are implemented in the industrial and smart cities domains at the global level[41]. This is as anticipated, since these two areas were the ones that attracted the most interest since IoT came into the scene of ICT.

[37] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[38] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[39] https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-_Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf

[40] https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf

[41] https://www.kontron.com/blog/embedded/iot-europe-losing-us

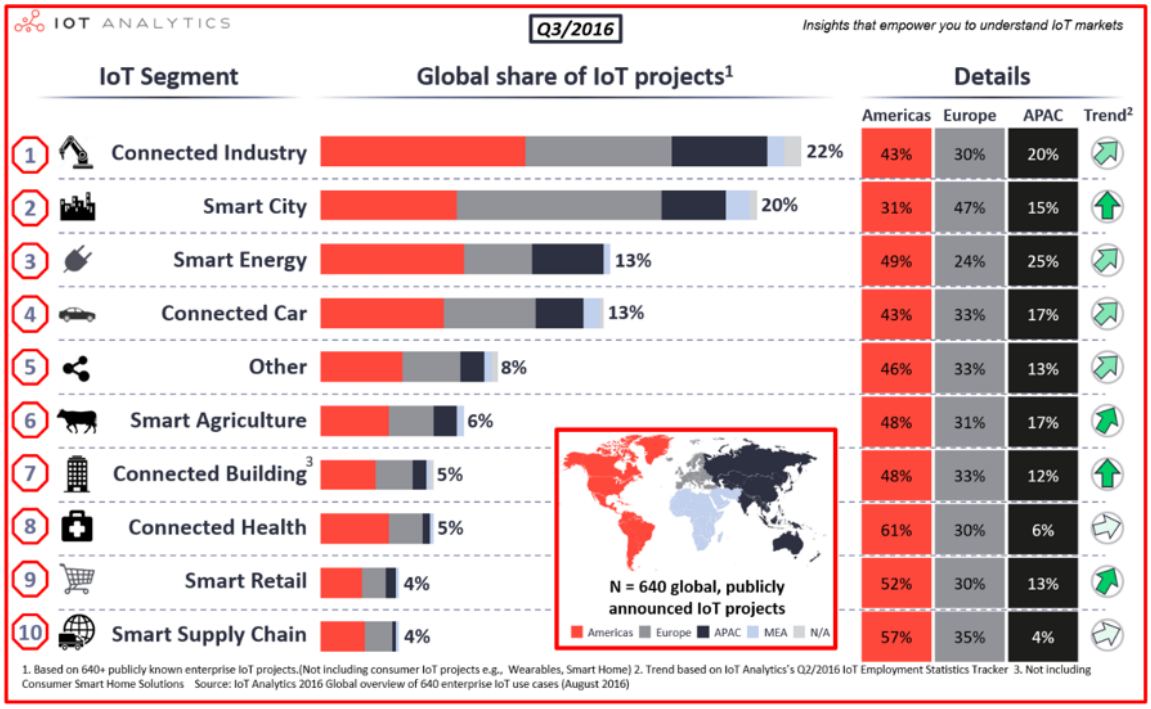


*Figure 3. Global share of IoT projects*[42]

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)[43].

The US is mostly focusing on developing advanced manufacturing and transportation systems with IoT, with these two domains being the dominant ones from the project's implementation point-of-view even, as part of the national IoT Strategy supported by the "Developing Innovation and Growing the Internet of Things - DIGIT" action that was introduced in 2016.[44]

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, since the AIOTI initiative was launched in 2015 with main objective of creating an industry-driven IoT ecosystem[45]. As regards 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. On the

[42] https://iot-analytics.com/top-10-iot-project-application-areas-q3-2016/
[43] https://www.inkwoodresearch.com/reports/global-narrowband-iot-market-forecast-2019-2027/
[44] https://www.slideshare.net/futurewatch/future-watch-chinas-iot-ecosystem-update-87972342
[45] https://www.slideshare.net/futurewatch/future-watch-chinas-iot-ecosystem-update-87972342

other hand, in the United States, the concept of smart urban space has been the main focus of the majority of successful start-ups[46].

For the Asia Pacific area, there is also a high degree of activity in the connected industry domain. 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.

## 4.2. 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, 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[47]. 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].

## 4.3. Micro- and macro-economic impact

IoT influences the economy on both the macro- and micro-economic level. From the macroeconomic perspective, we need a good proxy for investigations. 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[48] (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.

[46] https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/aig-white-paper-iot-june2015-brochure.pdf
[47] https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf
[48] https://www.frontier-economics.com/media/1167/201803_the-economic-impact-of-iot_frontier.pdf

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 implementation of IoT across, and between, several domains will have significant implications at 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 further enhance sophisticated decision-making processes. The effective handling of big data is of utmost importance, as it has the potential to enable noticeable savings in costs and significant reduction in waste production, as well as to transform the cost of asset ownership, improve capital allocation and overall efficiency. Furthermore, real-time, automated decision capabilities can be developed on top of these improvements. These enablers represent the key value creation aspects that IoT introduces to the production process and are expected to generate significant value at the microeconomic level through increased profitability. Consequently, companies are likely to face strong incentives to introduce IoT-related systems in their production systems, to distinguish themselves from competitors. One potential caveat related to the introduction of IoT in production lies in the exclusion of SMEs from IoT systems implementation due to the initial upfront cost that SMEs might not be able to bear. 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.

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

## 4.4. Application domains from the economic side

To provide more details about the specific impact, transformation potential and consolidated opportunities related to the exploitation of IoT technologies from an economic perspective[49], we select the domains where IoT technologies have the highest economic impact and where the transformation of the current business models is most remarkable. We discuss the following domains:

- **Energy Management:** IoT technology can be employed to create smart grids that price and route power, based on demand, and to prevent blackouts. The outputs from the sensors can be analysed by big data algorithms, used for machine learning and AI, which will lead to optimisation of resources and better service. Big data analytics, especially of renewable resources are of high importance for the future and hence IoT implementation in this regard should be prioritised.

[49] https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf

- **Manufacturing:** IoT could be applied for predictive maintenance of machinery based on the sensor data collected. Another aspect is production line monitoring by sensors, which enables equipment utilisation optimisation based on the data collected. In addition, this would simplify the implementation of flexible and tailored demand-based manufacturing, which would lead to the transformation of the entire supply chain. IoT implementation would also help manufacturers increase business profitability and productivity of both humans and machines. Predictive analytics engines help to make future manufacturing plants more autonomous in terms of predicting and fixing potential disruptive issues, which could otherwise lead to significant losses.
- **Transportation:** predictive maintenance, traffic jam predictions, optimal route calculation and car tracking are some of the many ways through which the adoption IoT in transportation may lead to cost savings. In particular, logistics is an important driver for IoT solutions.
- **Smart Cities & Communities:** this is one of the domains, or rather the integration of many domains, where IoT has enormous potential. The monitoring and management of traffic and transportation systems, power plants, water supply networks, waste, buildings, community services and others provide a solid basis for the generation of accurate analysis and predictions, that may enable cost optimisation, effective allocation of resources, and more sustainable and inclusive cities. One of the objectives is to cover smaller and rural communities, which would require more focus on the local ecosystem and the inclusion of citizens in the new digital ecosystem.
- **Healthcare:** the introduction of IoT in healthcare supports several scenarios, such as: hand hygiene monitoring systems, remote health monitoring through wearable devices, and smart medical apparatus manufacturing. The combination of smart sensors and cloud computing can optimise the flow of patients, staff, equipment and medical supplies hospital-wide. This gives many opportunities for the extension of revenue streams in the healthcare industry. Given that the optimisation is based on dynamic data, it can effectively reduce inefficiencies and enable better allocation of financial resources. Biometric wearables to track health and lifestyle provide important information concerning tailored medical treatment as well as reliable data for health insurance companies. New trends include the individualization of health care and preventative wellness programs based on the data analysed from wearables. An additional dimension is the improvement of the occupational health and safety of the workforce.
- **Smart Food & Farming:** IoT technologies enable crop control, remote monitoring of livestock, data collection about soil, crop and cattle conditions and it reduces human intervention (and thus labour costs) in favour of automated farming. The analysis of collected data may help to optimise farming and hence save costs and/or increase revenues. In particular, the progress in agriculture has been sector dependent - arable (mostly driven by sensors), dairy (IoT for cows and milk analysis and control), fruits (with diverse challenges in the field to assure high quality of the produce), vegetables (massive sensing and automation inside the greenhouses), meat (diverse IoT devices to ensure animal welfare as well as quality of the meat), aquaculture (a highly automated environment, that includes aquaponics). Farms are usually SMEs which have challenges associated with implementing IoT. The food chain has also direct relations to manufacturing of processed food, transport of produce, retail of

food in the smart city and possibly even urban farming. Another contribution is the traceability of food. There is a very strong opportunity for a cross-sectorial discussion

- **Retail:** the most important changes overcome by the implementation of IoT technologies are smart shelves, in-store layout optimisation, automated checkout, personalized discounts and the overall optimisation of the supply chain.

With respect to consolidated domains, new domains are emerging as relevant sectors benefiting from the adoption of IoT technologies. These emerging domains include:

- **The 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, thus boosting profits.
- **Insurance:** 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 and 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. One important aspect is company insurance for SMEs.
- **Safety and Defence:** the introduction of IoT in this domain can provide police officers and first responders with more efficient operations at lower costs, provided the IoT solutions are reliable and the upfront investment for their implementation does not face an excessive payback period. This can have high societal impact, for example, by improving the statistics of rescues and by increasing the detection of unexpected sources of risks upfront.

## 4.5. 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. By supporting SMEs and start-ups, Europe

can limit market monopolisation by the major and well-established players and at the same time strengthen European innovation in IoT domains.

- **Accurate economic parameters estimates (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, 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.

# 5. POSITIONING IOT WITHIN THE NGI: THE R&D PERSPECTIVE

## 5.1. R&D drivers for Next Generation IoT

As discussed in Section 3, 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 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.
- **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.
- **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'[50], adding the human-centred perspective and sensing/actuating capabilities in the human-objects-systems interaction[51]. 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.
- **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.

## 5.2. 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,

[50] https://aioti.eu/wp-content/uploads/2018/09/AIOTI_IoT-Research_Innovation_Priorities_2018_for_publishing.pdf
[51] 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

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.

### 5.2.1. 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.

### 5.2.2. 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.

The survey also highlights how responders think that the European Commission should sustain such development focusing on Large Scale Pilots, linked to further scale-up.

## 5.3. Priority application domains - the R&D perspective

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 4, 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)<br>• Real time decision making for IoT (R6)<br>• 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. |

| Domain | Top Related Research Priorities | Description |
|---|---|---|
| Healthcare | • Future-proof trust and security (R3)<br>• Human-in-the-loop IoT (R8)<br>• 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)<br>• 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. |
| Manufacturing | • Reliable, low-cost, sustainable and scalable sensor networks (R1)<br>• Next Generation IoT data processing architectures (R2)<br>• Real time decision making for IoT (R6)<br>• Autonomous IoT solutions (R7)<br>• Future proof trust and security (R3)<br>• Human-in-the-loop IoT (R8)<br>• 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)<br>• Human-in-the-loop IoT (R8)<br>• 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. |

| Domain | Top Related Research Priorities | Description |
|---|---|---|
| Insurance | • Real time decision making for IoT (R6)<br>• Human-in-the-loop IoT (R8)<br>• 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)<br>• Next Generation IoT data processing architectures (R2)<br>• 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. |
| Safety & Defence | • Reliable, low-cost, sustainable and scalable sensor networks (R1)<br>• Next Generation IoT data processing architectures (R2)<br>• 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)<br>• Real time decision making for IoT (R6)<br>• IoT & Data Semi-automated Interoperability (R4)<br>• Human-in-the-loop IoT (R8)<br>• IoT Data Sharing and Monetisation enabling models and technologies (R9)<br>• 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.<br>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.

# 6. LOOKING AHEAD - PRELIMINARY CONCLUSIONS

As highlighted by the economical, societal and research challenges discussed in Section 4 and 5, 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 4 and Section 5.

## 6.1. 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)

## 6.2. 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).


# NEXT GENERATION INTERNET OF THINGS

WWW.NGIOT.EU

NGIoT has received funding from the European Union's Horizon 2020
research and innovation programme under grant agreement N° 825082