ROADMAP FOR IoT RESEARCH, INNOVATION AND DEPLOYMENT IN EUROPE 2021-2027

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

Deliverable number	D3.3
Deliverable title	IoT research, innovation and deployment priorities in the EU. White Paper (Published as: "Roadmap for IoT Research, Innovation and Deployment in Europe 2021-2027")
WP number	WP3
Lead beneficiary	Archimède Solutions SARL
Deliverable type	Report
Dissemination level	PU
Delivery due month	M33
Actual submission month	M39
Authors	Francisco Molina Castro, Federico M. Facca, Adriënne Heijnen, Anna Brékine, Francesco Capparelli, Martin Brynskov
External Contributors	Ulrich Ahle, FIWARE Foundation; Gaël Blondelle, Eclipse Foundation; Jan Höller, Ericsson; Marco Jahn, Eclipse Foundation; Nuria de Lama Sanchez, Atos; Rute Sofia, Fortiss GMBH; John Soldatos, Intrasoft International; Ovidiu Vermesan, SINTEF Digital; speakers and participants at the NGIoT workshops 2018-2021.
Internal reviewers	Francesco Capparelli, IIP; Srdjan Krco DunavNET
Document version	2.0
Project start date	01.11.2018
Project end date	31.10.2021
Duration in months	36 months

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

Executive Summary

The "IoT research, innovation and deployment priorities in the EU White Paper" presents the project's final recommendations. The priorities and the linked roadmap were built based on the aligned work inputs from NGIoT different work packages and tasks, including the outcomes of the various stakeholder engagements, such as the series of workshops on IoT and Edge computing, and workshops addresseing other relevant themes, the NGIoT Strategy Board, surveys, and a series of indepth interviews with industry representatives,

Key priorities are classified into "Economic and Societal priorities", "Research, Innovation and Deployment" and "Strategic" priorities, as identified by several stakeholders along the Roadmap development. Industry specific priorities gathered from the latest workshops are also described to derive the specific recommendations for the different European research, innovation and deployment programmes.

Recommendations for the Horizon Europe programme

- **Data value**: Increase focus on IoT generated data covering architectures and business models, and boost research on data processing at the software and hardware stacks.
- **IoT Networks**: Ensure development of reliable, low-cost and scalable IoT networks, with reduced energy impact. Support experimentation and deployment.
- **Foster cost-efficiency of solutions**: Apply automatic approaches to govern IoT infrastructures, while researching semi-automatic approaches process interoperability to reduce the cost of the management of complex IoT platforms.
- **Data Management**: Foster transition from data management to insight generation, while enabling unified data processing from cloud servers to embedded processing units
- **IoT / Edge Operating Systems**: Go beyond "meta" Operating Systems, focusing on semi-autonomous orchestration. In the long run, move from centralised orchestration towards decentralised coordination with AI developments to increase autonomy.
- **IoT integration with other technologies**: Leverage the advancements in Artificial Intelligence, Distributed Ledgers and other technologies to evolve IoT platforms by introducing dynamic orchestration of processes.
- **Machine-human interaction**: Prioritise multidisciplinary research on machine-human interaction, including augmented reality, digital twins, tactile internet, while targeting a sustainable IoT-by-design approach.
- **IoT trials**: Support large deployments & experimental infrastructures beyond the covered by the Large Scale Pilots.
- **Future-proof security and privacy**: Develop security and privacy by-design to deal with future threats, increasing traceability and trust beyond regulatory compliance.
- **Green and sustainable IoT hardware**: Develop IoT miniaturisation, energy harvesting and pervasiveness while ensuring environmental compatibility.
- **IPR protection and patent promotion**: Enhancing IPR and marketing support for research projects to apply for patents, covering IPR costs for research and innovation.
- **Project impact promotion and assessment**: Increase the impact of relevant calls by adapting the process to reduce time-to-market from research project to marketeable products and services.

- **Cascade Funding**: Encourage cascade funding in IoT-Edge-Cloud calls to engage with new companies, SMEs and start-ups.

Recommendations for the Digital Europe Programme

- **Secure and Ethical IoT**: Support initiatives that increase trust in IoT adoption through cybersecurity and privacy-by-design, as well as enhance understanding of ethics and privacy, by deploying at large scale state-of-the art solutions for IoT services cyber-security.
- **Data models for interoperability and replicability**: Sustain the development and uptake of cross-domain harmonised data models, following the path established by OASC with the MIMs, to increase IoT application interoperability and replicability.
- **Innovation transfer**: Transfer the experience matured by running LSPs in Smart Cities, Agriculture and Healthcare to a wider set of actors through joined innovation procurement and similar actions.
- **Scalability**: Deploy secure and highly scalable IoT and digital infrastructures with special focus on edge capacity, leveraging on global networking technologies such as IPv6 and 5G.
- **Sustainability**: Leverage the potential of IoT for sustainable development in line with the UN Sustainable Development Goals, and societal needs and demands.
- **Independence and sovereignty**: Contribute to the technological independence of the EU in IoT critical infrastructures by increasing the scale and availability to EU citizens, with common and free access to data standards and secure-by-design IoT services.
- **IoT skills development**: Developing (Upskilling) and keeping (Reskilling) the right talent whilst leading in niche areas to compete in the worldwide landscape.
- **Open Innovation**: Develop open source IoT/Edge platforms that are more ubiquitous, pervasive, scalable, autonomous, light and sustainable. New research projects should use/extend/adapt existing open source platforms when they already exist.
- **Cooperation and standardisation**: To enhance cooperation among all IoT related organisations and fora to maximise the synergies, to reduce fragmentation of the European IoT community, and to increase harmonisation of IoT cloud-edge standards. The IoT Market will be shaped by global standards.
- **Large-scale research infrastructure**: leveraging and synergizing existing infrastructure (i.e., SLICES, Fed4FIRE+, etc.) and scalable platforms (i.e., GAIA-X, FIWARE, etc.) to create an European-wide infrastructure used by the projects.

Recommendations for the Connecting Europe Facility 2 programme

- **Computational power**: Facilitate access to large computational facilities needed to harness the complexity of analysing terabytes (or petabytes) of IoT generated data and ensure sovereignty by deploying digital infrastructures across Europe.

Abbreviations

3GPP	3rd Generation Partnership Project
5G-PPP	5G Infrastructure Public Private Partnership
5G-ACIA	5G Alliance for Connected Industries and Automation
5GAA	5G Automotive Association
ACEA	European Automobile Manufacturers Association
ACEI	Alliance for a Competitive European Industry
AI	Artificial Intelligence
AI2	Advanced Institute for Artificial Intelligence
AII	Alliance of Industrial Internet
AIOTI	Alliance for Internet of Things Innovation
API	Application Programming Interface
BDVA	Big Data Value Association
BPMN	Business Process Modeling and Notation
CCC	Climate Chain Coalition
CDBB	Center for Digital Built Britain
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
COSME	The EU programme for the Competitiveness of Small and Medium-Sized Enterprises
CMU	Capital Markets Union
CNCF	Cloud Native Computing Foundation
CPS	Cyber-Physical System
D	Deliverable
DEI	Digitizing European Industry
DIHs	Digital Innovation Hubs
DIN	German Institute for Standardisation
DKE	German Commission for Electrical, Electronic & IT of DIN and VDE
DLT	Distributed Ledger
EC	European Commission
ECCP	European Centre for Certification and Privacy
EECC	European Edge Computing Consortium
ECS	Electronic Components and Systems
ECSO	European Cyber Security Organisation
EFFRA	European Factories of the Future Research Association
EIB	European Investment Bank
EIP on AHA	European Innovation Partnership in Active and Healthy Ageing
EIP-SCC	European Innovation Partnership on Smart Cities and Communities
ENISA	European Union Agency for Cybersecurity
ENoLL	European Network of Living Labs

EPoSS	European Technology Platform on Smart Systems Integration
ESFRI	European Strategy Forum on Research Infrastructures
ETP4HPC	European Technology Platform for High-Performance Computing (ETP4HPC)
ETSI	European Telecommunications Standards Institute
EU	European Union
EuroXR	European Network for Virtual Reality, Augmented Reality and Mixed Reality
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GSMA	GSM Association
HL7	Health Level Seven International
HMI	Human Machine Interaction
ICT	Information and Communications Technology
IDSA	International Data Spaces Association
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIC	Industrial Internet Consortium
IMIA	International Association of Engineering Insurers
INATBA	International Association for Trusted Blockchain Applications
IoF2020	Internet of Food and Farm 2020
IoT	Internet of Things
IOTAC	IoT Acceleration Consortium
IP	Intellectual Property
IPR	Intellectual Property Rights
ISF	Information Security Forum
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union
ISO	International Organisation for Standardisation
LSP	Large-Scale Pilots Programme
M2M	Machine-to-Machine
NFV	Network functions virtualisation
NGI	Next Generation Internet
NSB	National Standards Body
OASC	Open & Agile Smart Cities
OMG	Object Management Group
RAMI	Reference Architectural Model Industrie
SDN	Software-defined networking
SDG	Sustainable Development Goals
SDO	Standards Developing Organisation

SLICES	Scientific Large-scale Infrastructure for Computing / Communication Experimental Studies
SME	Small and Medium-sized Enterprise
SRIA	Strategic Research and Innovation Agenda
SWOT	Strengths, Weaknesses, Opportunities, Threats
URLLC	Ultra Reliable Low Latency Communications
VC	Venture Capital
W3C	World Wide Web Consortium
WFO	World Farmers Organisation
WG	Working Group
WIPO	World Intellectual Property Organisation
WP	Work Package

Contents

List of Figures

List of Tables

1 INTRODUCTION

As digital technologies increasingly embrace all parts of society and industry, the digital and physical world are entangled in new complex ways. The Internet of things (IoT) and the recent developments on Edge computing are narrowing the gap between the virtual and physical worlds. While this lays the ground for further virtualisation, the fact that such pervasive virtualisation takes place, literally, generates a very real push-back from the physical side. The complementation and collaboration of both worlds in an ethical and sustainable way is necessary as we move towards a sustainable and smart future. Europe is committed to pursuing and achieving ambitious sustainability targets as part of a twin green-digital transformation of society, including of industrial enterprises and other organisations. In this context, the IoT-enabled convergence of the physical and digital worlds provides opportunities for realising the digital and green transformation of European organisations. Similar to the way the previous decade (2010-2020) acted as a catalyst for the digital transformation of European enterprises, the present decade (2021-2030) is expected to drive and accelerate this twin transformation, while insisting on delivering a sustainable future for its citizens, meaning both green, prosperous and inclusive, while at the same time guaranteeing security and autonomy.

Within this paradigm shift, Europe must take advantage of the decentralisation trend through new IoT and Edge Computing capabilities, and leverage the expertise of its communities in the physical, industrial world to bring the best of both worlds.

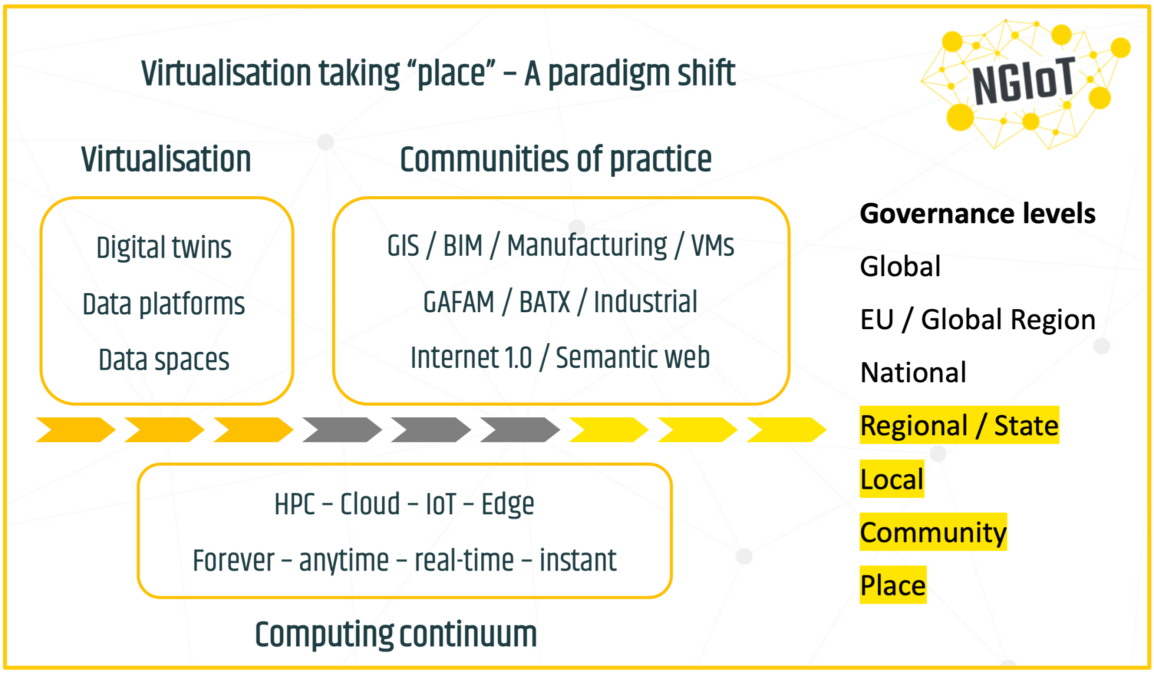

Figure 1. Paradigm Shift: Virtualisation taking place (Brynskov, 2021)

This whitepaper was developed by the NGIoT Coordination and Support Action, a consortium of partners (NGIoT Consortium, 2018), in cooperation with different European and Worldwide organisations, and various stakeholders from the academia and industries relevant to the project. The roadmap was enriched through a set of activities, including, but not limited to, surveys, interviews, a series of workshops and other consultation efforts and, thus, this whitepaper focuses on insights from and for the IoT and the Edge computing communities.

1.1 Scope - Why this CSA R&D&I priorities whitepaper?

The “IoT research, innovation and deployment priorities in the EU White Paper” aims at synthesising insights from key resources in the complex and wide area of IoT as input to the European Commission (EC), EU member states and other stakeholders when shaping upcoming initiatives, including research, innovation and implementation programmes in the EU Multifinancial Framework (MFF). It particularly, but not only, intends to provide a set of priorities through an IoT R&D&I Roadmap based on market needs, the European context and the state of the art, for the Horizon Europe and Digital Europe programmes. The roadmap emerges from the 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. Given the evolution of technology during the implementation of the different activities of NGIoT, the paper integrates the role of Edge computing as it is a key part of the IoT ecosystem[1].

Nowadays, the Internet is an integral part of our lives and business. We can exploit the opportunities it creates, but we have to be aware and mitigate the risks at the same time. In order to support these activities, Europe aims to re-invent the next generation of the Internet by “shaping a value-centric, human and inclusive Internet for all” (NGI.eu, 2019). We can name the Next Generation Internet (NGI) initiative launched by the Digital Single Market of the European Commission (EC) in autumn 2016, with the goal to contribute to creating a ‘highly adaptive and resilient’, ‘trustworthy’ and ‘sustainably open’ human-centric Internet.

The strategy for a successful implementation and exploitation of IoT in all economic areas is based on three main pillars: a **thriving IoT ecosystem**, a **human-centred IoT** approach and a **single market for IoT**[2]. In March 2015 the Alliance for the Internet of Things (AIOTI[3]) was set with the goal to coordinate ongoing activities and set a direction for the full exploitation of opportunities created by IoT. IoT is regarded as a key component and challenge towards the ‘Digitising European Industry’ strategy and the Next Generation Internet of Things. It brings transformation from the economic, business and societal point of view. The Internet of Things (IoT) is involved in various highly impactful application domains, ranging from healthcare and agriculture to industry and leisure. Also, the EU invested almost EUR 500 million in IoT-related research, innovation and deployment under Horizon 2020 for the period 2014-2020.

IoT is also crucially tied to advancement in other fields such as cloud computing, AI, Human Machine Interaction (HMI), Big Data and data analytics, Quantum Computing, 5G (Road2CPS Technology and Application Roadmap). It is the key driver of the Big Data phenomenon due to its ability to connect a variety of smart devices or objects which generates a growing amount of data, according to the Strategic Research and Innovation Agenda (SRIA[4]).
The European Commission has published several strategic documents. Of central relevance are: Europe Fit for the Digital Age[5]; Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030[6]; A New Industrial Strategy for Europe[7]**;**

---

[1] IoT and Edge Comouting: opportunities for Europe, NGIoT, November 5, 2021, https://www.ngiot.eu/report-iot-and-edge-computing-opportunities-for-europe-2/

[2] https://digital-strategy.ec.europa.eu/en/library/digitising-european-industry-initiative-nutshell

[3] https://aioti.eu/

[4] https://www.eosc.eu/sites/default/files/EOSC-SRIA-V1.0_15Feb2021.pdf

[5] EC, European Commission. (2020). *A Europe Fit for the Digital Age*. Retrieved from https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en#latest

[6] EC, European Commission. (2021). *Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983

[7] EC, European Commission. (2020). COMMUNICATION. A New Industrial Strategy for Europe. https://ec.europa.eu/info/sites/default/files/communication-eu-industrial-strategy-march- 2020_en.pdf

Rethinking strategic autonomy in the digital age[8], further strengthening 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, The European Green Deal[9]as well as the commitment to defend European digital autonomy, sovereignty and security[10].

With the mission-oriented Horizon Europe and Digital Europe vision, complemented by structural funds and private investments, Europe has laid out the tracks to tackle this complexity, to the benefit of European citizens, and beyond. As the new Commission was announced, the focus on digital and the link to the digital single market was emphasised, including Commissioner-designate Executive Vice President Margrethe Vestager giving the portfolio title "a Europe fit for the Digital Age"[11]. This marks a level of ambition and a strategic integrated approach to technology, market creation and competition not seen before. The NGIoT scoping paper, the NGIoT Market Research and Business Modelling study, and the report on IoT and Edge computing[12] and this Strategy Roadmap should be seen in this light, supporting directly this ambition of the EC and providing a guidance for the identification of the key research and innovation topics and how to address them.

1.2 Main goals

This white paper aims at supporting the European Commission, EU Member States and other stakeholders to:

- Prepare for and lead the development of next generation IoT and it relationship to Edge Computing, 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).
- Guide the need of EU's digital capacities technologies related to IoT-Edge Computing (data, cybersecurity, AI, skills, interoperability etc.) in industry and the public sector.
- Support the Digital Single Market vision, linked to prosperity on the local community-level.
- Understand strategies to maximise societal, economic and environmental benefits of IoT-Edge Computing, including roll out and adoption.
- Explore the role of cross-technology challenges like Cybersecurity and Privacy-by-Design technology within the IoT-Edge Computing ecosystem addressing end-user acceptance.
- Strengthen and further mobilize the European IoT community and ecosystem.

---

[8] EC, European Commission. (2019). *Rethinking strategic autonomy in the digital age.* Retrieved from https://op.europa.eu/en/publication-detail/-/publication/889dd7b7-0cde-11ea-8c1f- 01aa75ed71a1/language-en/format-PDF/source-118121846

[9] EC, European Commission. (2019). *What is the European Green Deal?* Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/fs_19_6714

[10] EC, European Commission. (2019). *Rethinking strategic autonomy in the digital age.* Retrieved from https://op.europa.eu/en/publication-detail/-/publication/889dd7b7-0cde-11ea-8c1f- 01aa75ed71a1/language-en/format-PDF/source-118121846

[11] EC, European Commission. (2020). *A Europe Fit for the Digital Age*. Retrieved from https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en#latest

[12] IoT and Edge Comouting: opportunities for Europe, NGIoT, November 5, 2021, https://www.ngiot.eu/report-iot-and-edge-computing-opportunities-for-europe-2/

1.3 How to read this document

The main contribution of this document to address the objectives mentioned in the previous section can be found within chapters 5 and 6. Readers who are already familiar with the general concepts of IoT-Edge Computing and the European IoT-Edge Computing landscape are advised to put emphasis in those two chapters as the previous ones build up the context to conclude the information within them.

Readers that wish to understand the technology context of this document can address Chapter 2 as a way to understand some of the basics of the topics addressed afterwards. Those readers who are already familiar with the concepts, but wish to understand the European context and the sources of input for the conclusions, can address chapters 3 to 4, as they contain most the work done to get to the final priorities, challenges, recommendations and conclusions.

1.4 Methodology

The work leading to this white paper has been organised to create and deliver meaningful insights and recommendations for several stakeholders surrounding the IoT and Edge computing communities, including public and private investments, policy makers and those with an interest in the outlook for IoT and Edge computing development in the European landscape.

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.

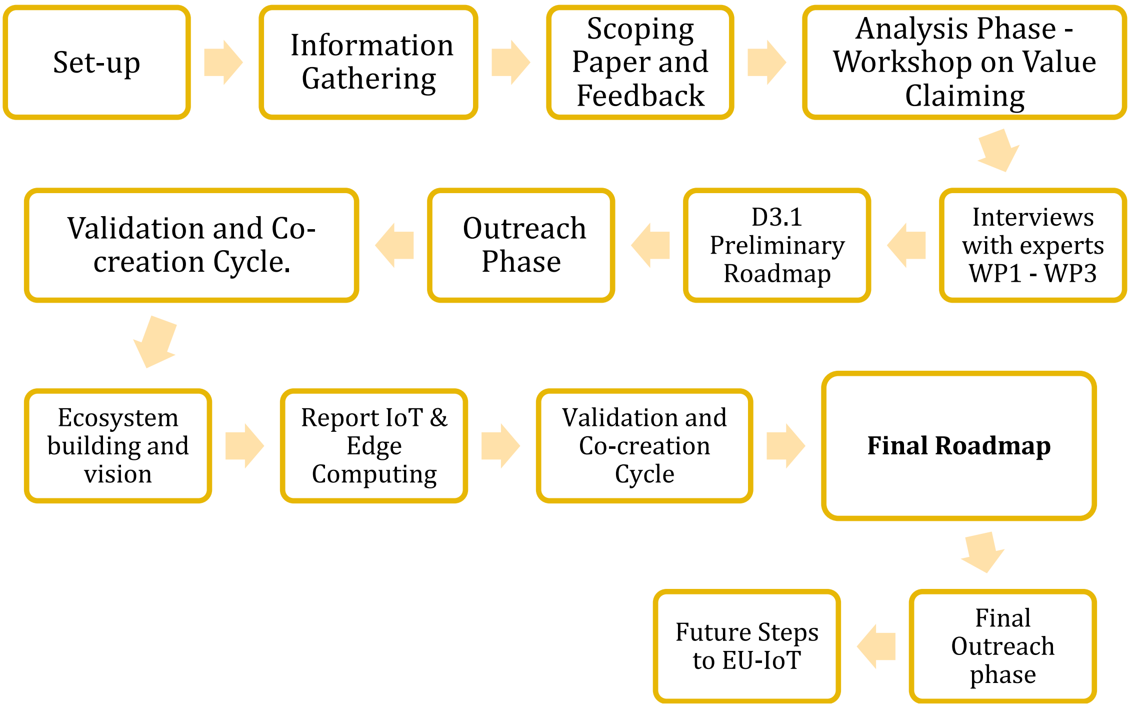

Figure 2. WhitePaper Methodology and Future steps to EU-IoT[13]

The work was organised as follows, while complemented with the different activities exposed in Figure 2. WhitePaper Methodology:

- **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 stakeholder, communities and 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, including, but not limited to, industry strategic agendas like the Artemis ECS

[13] https://www.ngiot.eu/eu-iot-project-kicks-off/

Strategic Research and Innovation Agenda of 2021[14], and the Networld SRIA, articles related to IoT from various organizations like the OECD reports and the initiative like Digital Europe, as well as position papers related to IoT as well as the identified technology dirvers. Additional resources include material presented at the kick-off meeting and at dedicated events, such as the IoT Week, the Digital around the world event and several online workshops on a variety of topics.

  - Stakeholder and expert input from targeted dialogues/interviews online (NGIoT Consortium, 2020) as well as at relevant IoT conferences, workshops and webinars.
  - 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.
  - NGIoT workshop series including the NGIoT thematic workshops (Energy, Smart cities & communities, Health and Care, Manufacturing and Agrifood), the IoT and Edge I and II (The far edge), the IoT and Edge Computing Future Directions and the IoT and Standardisation workshops [15]

- **Analysis Phase**. Information collected from the various sources in the previous phase 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, Industry experts and several EC representatives, and was partly done during the same workshops from the information gathering phase. This allowed to build over the original scoping paper, the Initial IoT research, innovation and deployment priorities in the EU white paper, and the Edge Computing report, to conclude with the current document.
- **Outreach Phase.** The white paper will be widely distributed and promoted across the various NGIoT channels, after the final round of validation with the EC in the last months of the project. This will be the basis for further consultation and co-creation processes, run in conjunction with the NGIoT Strategy Board, expert groups and other stakeholders. The information in this document is synthesised to help define the scope of the future research, innovation and implementation priorities for the European Commission, member states and other stakeholders considering the relevance and potential of the various challenges ahead.

1.5 Inputs from the community

This deliverable integrates efforts from different sources, enriched by desktop research and enhanced thorugh iterative consultations as described in the previous section. NGIoT inputs derive specifically from the scoping paper surveys, strategy board, other surveys and

[14] https://artemis-ia.eu/documents.html

[15] https://www.ngiot.eu/archive-ngiot-resource/

interviews, and the thematic workshops. The two most notorious sources of input include the strategy board approach and the different workshop series.These inputs were integrated within this document, mostly in Chapters 4 and 4.

1.5.1 Strategy Board Approach

The Strategy Board has been crucial in this development, gathering experts in IoT from various backgrounds and representing IoT related alliances, organizations, industry and academia. The NGIoT Strategy Board met regularly to comment on various working papers produced by the NGIoT consortium, as the scoping paper and the IoT roadmap. Among the most important inputs included measures to maximize the economic and societal impact of European research on IoT for European industry and citizens (NGIoT Consortium, 2021), and activities like the *"Workshop on European Research Support and Contribution to Global Standardisation, Internet of Things Perspectives"* at the International Telecommunication Union (ITU) in Geneva, the *"Workshop on Value Claiming"* in Crans Montana, Switzerland, and the most recent virtual "*Workshop on IoT and Edge Computing Research and Standardisation Convergence"*.

Out of this efforts, the Strategy Board helped enhancing integrally various topics across this document, to mention the SWOT analysis to enhance the market research report and the strategic recommendations

1.5.2 Thematic Workshops

In addition to the meetings of the NGIoT Strategy Board described above, NGIoT has reached out to a broader community of experts through organising workshops and webinars on specific topics and emerging trends. To achieve a larger impact and mobilise the ecosystem, the workshops have been organised in conjunction with already existing networks and events and in collaboration wth other key players.

The webinars and workshops organized so far have ranged broadly from edge computing, far edge, industry specific workshops, human-centred IoT, to cybersecurity, reference architectures, standards and privacy by design. The discussions and presentations during the workshops and webinars confirm the importance of the research challenges and topics that have been identified in the draft IoT Roadmap for Research, Innovation, and Deployment and are presented in this deliverable. The webinars and workshops also provided important information not only for this document but to further shape the current proposed challenges and trends, as well as move into new directions, as described in NGIoT deliverable 3.2. Future Trends in IoT.

2 IOT AND EDGE COMPUTING FOUNDATIONS

2.1 IoT – Definition and Scope

It is important to clarify the understanding and reach of the different terms used in this document, the domains and drivers explored in the study and their relationship to IoT. Defining a technology is not easy: different stakeholders put accents on different aspects, or again, the definition of a technology may evolve over time with the evolution of the technology itself. This applies to the "Internet of Things" (IoT): its architecture, functionalities and goals today are surely not the same as when Kevin Ashton coined the term "the Internet of Things" in 1999 to link Radio-frequency identification (RFID) technology to the Internet (Ashton, 2009).

In 2015, the IEEE launched a community effort to "contribute to the ever changing definition of IoT" (IEEE IoT Technical Community, 2020), that resulted in the following definition:

> "*Internet of Things envisions a self configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration.*" (Minerva, Abyi, & Rotondi, 2015)

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

The International Telecommunication Union (ITU), one of the main Standard Development Organisations (SDOs) in the field, provide a more generic definition of IoT (ITU, 2012):

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

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

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

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

In short, we can define the Internet of Things as a systems of systems (Jamshidi, 2008) that have (at least) the following properties:

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

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

2.2 IoT Architecture

Several organisation and projects worked on the definition of reference architectures for IoT systems, including, for example, IoT-A (Bauer, 2013) and Large Scale Projects (EU LSP Programme, 2018), open source projects like WSO2 (Fremantle, 2015) and FIWARE (FIWARE, 2020), industrial organisations like AIOTI (AIOTI, 2020) and ICC, and standard development organisations like ISO (ISO, 2018) and ITU (ITU, 2019). Some of them, like the Industrial Internet Consortium (Shi-Wan, 2017), the Reference Architectural Model Industrie 4.0 (RAMI) (ZVEI, 2018) and Synchronicity (Synchronicity, 2019) are connected to specific domains. Defining a new reference architecture is out of NGIOT's scope. Large Scale Pilots have consolidated their effort in an interesting 3D reference model (cf. Figure 3) that combines architectural layers, non-functional properties and cross-cutting functions.

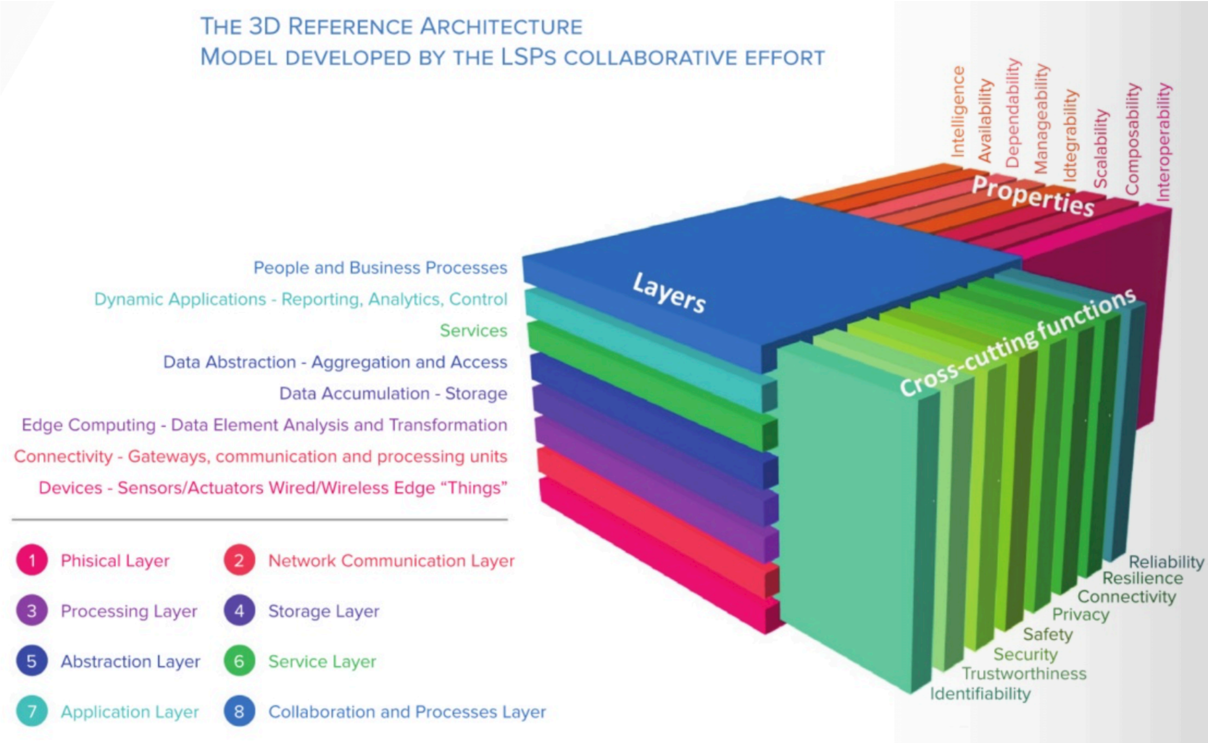

Figure 3. LSP 3D reference architecture

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

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

2.3 Edge computing – Definition and Scope

IoT solutions build on top of a computing and network infrastructure that by its nature is distributed. In the first IoT deployments computation was occurring mostly centralised (in the cloud) while sensor where collecting data at the edge. Increasingly, over the last few years, different scenarios show the limitations of a pure cloud-centric approach to service delivery platforms. Thanks to the evolution of devices at the edge of the network, that offer nowadays higher computational capacity, and to answer to the different needs (e.g. latency, privacy, reliability), posed by IoT applications, platforms and solutions enabling the processing of data at the edge of the network (where the data is generated) are arising on the market, realising what is called "edge computing". In many applications, the necessary computations are increasingly being carried out on spatially distributed devices, with computing generally done where it is most efficient (AENEAS, Artemis IA, EPoSS, 2021; ISO, 2020).

Edge Computing (ISO, 2020) is defined as "distributed computing in which processing and storage takes place at or near the edge", where edge "is boundary between pertinent digital and physical entities, delineated by networked sensors and actuators".

It is no mystery that several IoT scenarios are pushing and demanding for the adoption of Edge Computing. The latter is also propelled by the rise of other trends such as distributed ledger technologies, as well as other technologies for 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. Edge computing for solutions for IoT come at different flavours, including for example local processing within embedded computing platforms and processing in industrial gateways that interact with embedded devices. The latter is also known as fog computing. Clearly Edge Computing is not only an enabler for IoT but also for other technologies where computation at the edge enables novel capacities and application scenarios. Compared to other adoption scenarios, IoT may have specific requirements that edge computing needs to support.

Is Edge Computing a new thing? While solutions providing computation or storage at the edge of the network are around since years (such as Content Distribution Networks), edge computing is now seen as extension of cloud technologies. Edge computing is becoming the new computing layer located in the devices/embedded systems at the "edge of the network" provides computing abilities in a self-provisioning, API-based and monitorable way (like in the "cloud").

Recently, we also witnessed more and more the usage of the terms "near edge" and "far edge". The first definition is generally related to an infrastructure able to host generic services in a location between the far edge and the cloud data centres. A near edge infrastructures is not on premises and is often shared among multiple tenants. The term far edge refers to the edge infrastructure which is deployed closest to users in a location farthest from the cloud data centre. Far edge infrastructure is generally on-premise and not shared.

The increasing IoT requirements of real time data collection, process, analysis and actuation drive the development of optimal edge computing solutions. Gartner estimates that driven by IoT, data processing outside of the data centres will pass from 10% to over 75%[16]. Some of the worldwide initiatives and players:

- Cloud: Amazon AWS, Google Cloud, Microsoft Azure and IBM Cloud are the biggest cloud providers worldwide (Gartner, 2019), followed by Alibaba Cloud which plays the biggest role in China, whereas in Europe the landscape is more fragmented.

16 Gartner. What Edge Computing Means for Infrastructure and Operations Leaders (2018)

- Edge: as a fragmented and relatively young industry, the biggest players come from cloud providers and other knowledgeable companies. With Microsoft notably holding over 300 patents (Forrest, 2018), Amazon (Greengrass, FreeRTOS, Lambda@Edge), DELL CME, HPE, IBM Edge Computing and Cisco Edge and many other smaller companies play an important role. Edgeir provides an extensive company list (EdgeIR, 2021) with some big, medium and small players worldwide.

2.4 Edge Computing Architecture

Despite being a new area, several standards, researchers and open source initiatives are dealing with edge computing and defining architectures for its implementation. Often such architectures depict a combination of IoT and cloud technologies to deliver edge computing solutions. Clearly, a consolidation would be only possible after the wider adoption of edge computing, i.e. an increasing number of successful deployment of edge computing based solutions. Similar to the IoT Large Scale pilots, (Willner, 2020) proposes a 3D model lightinghing the characterizing aspects of edge computing architectures. The model highligths in particular the edge computing spatial hierarchy, ranging from the *product edge*[17] to the *public cloud*, and the architecture layers composing the edge computing infrastructure (such layers, with minor differences, map to the ones of Figure 3).

Figure 4. Reference Architecture Model for Edge Computing (Willner, 2020)[18]

2.5 IoT-Edge Application & Industry Domains

Nowadays, the range of IoT applications is very wide and covers an always enlarging set of domains. On a survey elaborated by KPMG, with over 750 tech leaders ranging from Fortune 500 executives to start-up entrepreneurs, respondents align towards pointing that IoT will drive the greatest business transformation across many industries in the next three years, bringing

[17] Product edge stands for a device product capable to provide computation, such as a smarth phone. In this sense, the product edge device is a far edge device.

[18] https://ecconsortium.eu/

benefits to life, society and the environment (KPMG, 2018). Because of the breadth of reach of IoT, the study selects the following industry domains of interest, basing the selection on the initial market analysis of the NGIOT scoping paper.

A more detailed perspective of the different domains supported by IoT applications is discussed in Section 4.1.3. The list in this section gives a first overview of the typical scenarios in the most relevant domains:

- **Agrifood and Smart Farming**: IoT is becoming an important instruments in agri and farming industry. The ability to measure in real time different aspects of crops and animal farms, allows for optmisation and automation of different processes such as watering, harvesting, and animal feeding.
- **Smart cities and communities**: IoT revealed as a key technology to monitor city (from environment to any other aspect, such as parking and waste) and to optimize resources (transports, water, energy, …) and ultimately increase quality of life of citizens. It's ability to provide KPIs and instrument to "measure" the city proved to be as well important in engaging citizens and increasing their awareness of their own city.
- **Smart Health**: IoT contributed to the evolution and innovation of the healthcare services. IoT have been successfully adopted to, for example: control drugs/medicines, increase automation in hospital management, individual health in real-time, track pandemies[19]
- **Energy Management**: Thanks to IoT, it is possible to montor the behaviours of electricity suppliers and consumers and, hence, improve the energy efficiency.
- **Manufacturing**: IoT enabled the machine-to-machine communication across the manufacturing plant, enabling real-time monitoring and control of the manufacturing processes. This ultimately allows to improve the quality of the production and its control leading to novel products and levels of product customisation on the market, while containing costs.
- **Automotive and Transportation**: Self-driving cars are becoming a reality thanks to IoT: different sensors are collecting the status of the car, and by leveraging on external data sources (e.g. real time traffic, maps, …), able to advice drivers, and to drive autonomously the vehicle.
- **Insurance and Finance**: enhancement of bank security and smarter interactions like contactless payments are some of the benefits IoT brings to the financial industry. Data gathering and personalized risk assesments are part of the innovations through IoT in the Insurance industry.
- **Smart Living**. IoT is contributing to a smarter living through both the macro and micro approach. Increasing quality of life with the automation of homes, energy saving and support for elder people.
- **Retail**. IoT proved to be a key technology to increase supply chain efficiencies, develop new services, and reshape the customer experiences. Typical applications include: tracking goods, real-time inventory, information exchange among suppliers and retailers, and automated delivery capabilities.

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

2.6 Key enablers for a Next Generation Internet of Things

The European landscape, further detailed in Section 4, is very active on evolving Internet of Things and related technologies and the European Commission, seeing it as central, supports a wide set of research a policies related to the area, including the Next Generation Internet initiative. A critical challenge for the upcoming years is the need to 'leverage EU technological strength to develop the next generation of IoT devices and systems' taking full advantage of the key enabling technologies of 5G/6G, trust and cyber-security, distributed computing, cloud architectures, Artificial Intelligence (AI), Machine Learning, and Advanced Computing 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 (European Commission, 2020).

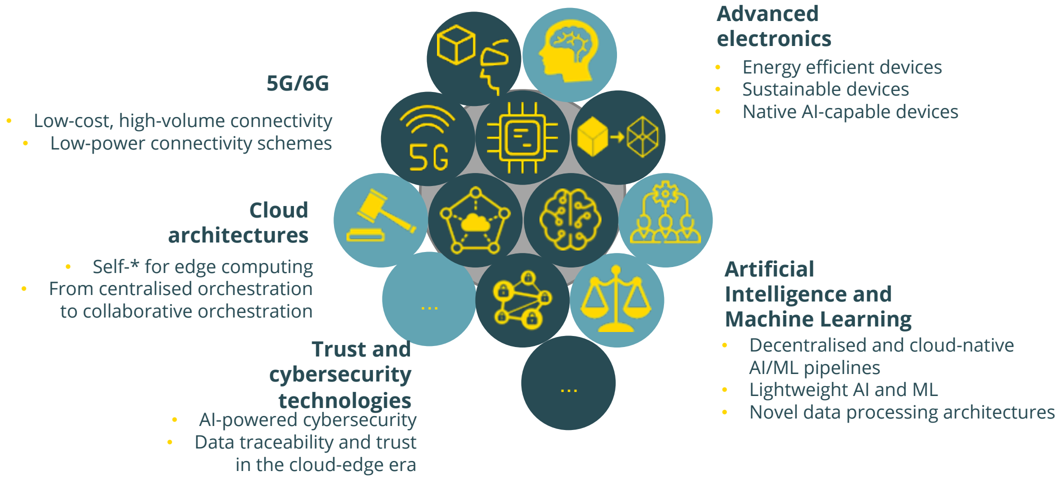

Figure 5. Key technology enablers and research areas to realised the Next Generation Internet of Things

In this context, key technology enablers for realizing the Next Generation Internet of Things have been identified as:

- **5G/6G**: This technology enabler refers to the new generation of mobile communication that supports a massive number of devices with a diverse range of speed, bandwidth and quality of service. The fifth generation of mobile cellular technologies encompasses reliability, latency, scalability, security and ubiquitous mobility. The 5G Observatory divides the service in 3 big scenarios according to the application needs (GSMA, 2019), Enhanced Mobile Broadband (EMBB), massive Machine Type Communications (MMTC) and Ultra Reliable Low Latency Communications (URLLC). MMTC promises to allow cheap, reliable and scalable internet connectivity, which is a key requirement for several IoT scenarios. With its augmented spectrum, 5G aims to tackle requirements posed by IoT large deployments beyond what today is possible with Low Power Wide Area Networks (LPWAN), achieving massive and critical communications with a complete vision deployed by 2021 (Nokia Bell Labs, 2019). Some of the worldwide initiatives and players:
  - Besides the 5G providers, McKinsey identified 3 main players poised to win: component suppliers, industrial automation companies and manufacturers (McKinsey, 2020). In terms of providers, the clear global players are Ericsson, Nokia and Huawei. As for the component suppliers, the providers vary withi EMBB, URLLC and MMTC, with Qualcomm, Skyworks, Intel, Broadcom and Xilinx (CNBC, 2019) as some of the top firms.
  - Even if Europe is lagging behind in 5G deployment for eMBB, it is playing a major role in the MMTC sector, thus exploiting its positioning to influence the

future of IoT infrastructures, which is a key opportunity for Europe to gain global leadership. It is calculated that in 2019 around 45% of the Smart City projects were done in the European Union, spending in 5G research and standards that drive areas like IoT and Machine-to-Machine (M2M) communication (Insight Partners, 2019). Europe has also the input from projects across several vertical domains where it has been determined that in most cases, the specifications of 5G fulfill the requirements for successful implementation of solutions across the Smart Mobility, Smart City, Smart Energy, Smart Agriculture, Smart Manufacturing and Smart Health verticals (AIOTI, 2019). Furthermore, cybersecurity and privacy remain two of the main concerns for Europe in this area (Open Access Government, 2020).

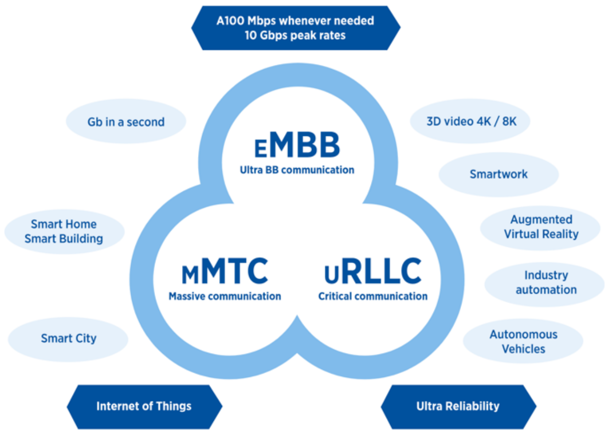

Figure 6. 5G Usage Scenario

- **Artificial Intelligence and Machine Learning**: Blended with IoT, AI offers augmented intelligence in the data analysis process. The availability of massive data sets to train, test and apply AI (Big Data[20]) combined with increasing High-Performance Computing (HPC[21]) capability enabled its wide adoption in several real-life scenarios. This combination is expected to kick off the next wave of performance improvements, especially in the industrial sector (McKinsey, 2017), by enabling extraction of unexpected 'intelligence' from sensed data, the automatic actuation based on 'intelligent' models (e.g. self-driving cars), the higher automation in the management of a plethora of devices and their generated data. Also, as Artificial Intelligence becomes a reality across several application (Novarica, 2017), its combination with IoT is moving towards the edge (i-scoop), enabling usage of algorithms closer to the devices. In fact, a study on Emerging Technologies in Electronic Compnents and Systems (DECISION Etudes & Conseil, 2020) identifies AI at the edge as one of the key opportunites for Europe.
  - The White Paper from the EC signals the landscape of AI in Europe (European Commission, 2018), describing Europe's current position of strength in digital competencies, research centres, innovative start-ups, and world-leading robotics and manufacturing with AI solutions. It also highlights Europe's potential and gives recommendations to leverage on these strengths, which promise to drive the complementarities of AI and IoT. Within these recommendations, focusing on SMEs and start-ups is also pointed out on a Roland Berger study, indicating

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

[21] InsideHPC. AI-HPC is Happening Now (2018)

that AI start-ups in the IoT area are weekly underrepresented in comparison with other regions (Roland Berger, 2018). As this combination has the potential to change business models, European businesses have to further embrace the opportunity to think strategically about AI and IoT instead of following shorter term goals (DIGITAL SME, 2020).

- **Cloud technologies:** while the increasing transition toward edge will reduce adoption of traditional cloud providers, the role of cloud technologies will be still key to enable scalable and autonomic IoT infrastructure spanning from cloud to edge (or across edges). Cloud-native approaches have been proved to work effectively also in distributed scenarios and to enable role out and automation of IoT services in the cloud-edge continuum. Evolutions of these technologies will be key to allow IoT to scale at the edge and across multiple infrastructure providers.
- **Hardware & Sensors:** the role out of edge computing clearly depends on the evolution of hardware. Edge nodes are requested to run AI and machine learning tasks that so far were only possible in cloud infrastructures, while dealing with other constraints such as energy capacity. The latest developments in microprocessor architectures and ongoing research (e.g. neuromorphic computing) should provide novel computing capacities able to support AI tasks not possible today at a lower energy footprint than today. The increasing number of deployed sensors will also impact IoT sustainability, thus demanding for - not only more energy efficient sensors - but as well more bio-compatible ones.
- **Cybersecurity:** the move from a centralised infrastructure to a distributed and decentralised one, - while clearly reducing the need to move data to third party infrastructures - it increases the complexity of security management and increases the potential surface of attack of the infrastructure. It is expected that security and privacy technologies will evolve to scale in a decentralised deployment and to increase their resiliency to novel mechanisms of attack that may compromise edges.

3 ECONOMIC OPPORTUNITY FOR EUROPE AROUND EDGE-IOT

NGIoT developed the "Market Research and Business Modelling" with the objective to provide an indepth analysis of the IoT market, IoT application domains, IoT-related emerging business models and technology enablers to help identify economic opportunities and challenges related to the research, development and implementation of IoT-related activities. The focus of the report is to align with the priorities and industry-needs, in order to serve as an input for the NGIOT Roadmap to enhance Europe competitiveness in the global market for IoT products. This section summarizes the economic projections section of the "Market Research and Business Modelling" report, available as Annex 2.

3.1 Market dimensions and segmentation

Studies from the different selected sources present a very positive projection with significant growth in the upcoming years for the IoT market (Hardware, Software and Services). Reports from IHS Markit (IHS Markit, 2018), Ericsson (Ericsson, 2018) and IoT-Analytics (IoT Analytics, 2018) show an estimated number of global connected devices ranging from **7 to 9 billion in 2017**, with projected growth from **15% to 30% Compounded Annual Growth Rate (CAGR)** depending on the industry, the geography and the type of connection. Variations across projections are due to different metrics and methodologies used to calculate the market potential. As for Edge computing specifically, Mckinsey positions the forecast to 2025 at a potential hardware value of $175B-$215B (McKinsey&Company, 2018), while the Linux foundation calculates an approximate global CAPEX of $146B for 2028 at an average CAGR of 35% (LFEdge, 2020), with a faster growth on the device edge.

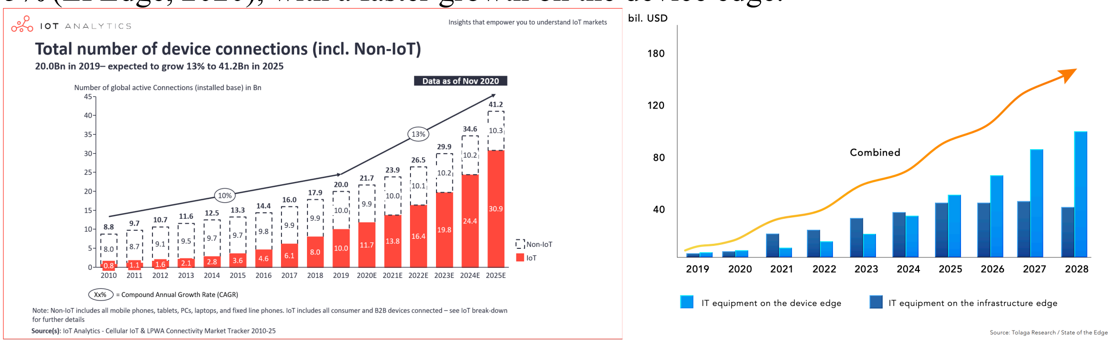

Figure 7. IoT [22] and Edge[23] global market estimations

Projections position North America dominating the Edge Computing market due to its high adoption of technologies such as IoT and 5G (IDC, 2020). Europe shows the second highest edge infrastructure investment by 2028 just behind APAC, which is the region with the highest growth rate (IndustryARC, 2020). The largest customers are Western Europe multinational network operators leading network upgrade efforts.

[22] https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/
[23] https://www.lfedge.org/wp-content/uploads/2020/04/SOTE2020.pdf

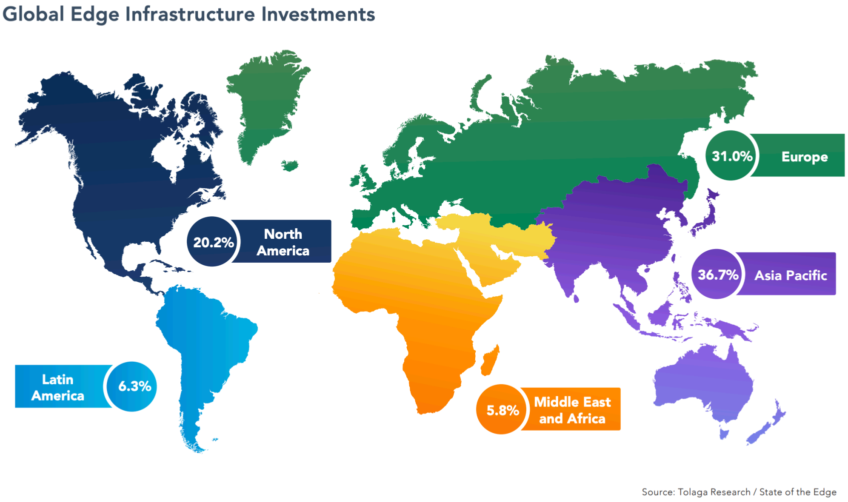

Figure 8. Global Edge Computing Infrastructure Investments

As for market value, projections from Bain (Bain & Company, 2018), EY (FICCI & EY, 2019), Mordor Intelligence (Mordor Intelligence, 2021) and IoT analytics (IoT Analytics, 2018) based their global IoT expenditure numbers ranging from **USD$1.1 Trillion to USD$1.5 Trillion by 2025**, with CAGRs that stay in the range of 10.5% up to 22%. Geographically, these projections position Asia-Pacific (APAC) as the biggest region in terms of volume, followed by North America and then Europe, the Middle East and Africa (EMEA). All of the studies classify EMEA as the region with the highest relative growth.

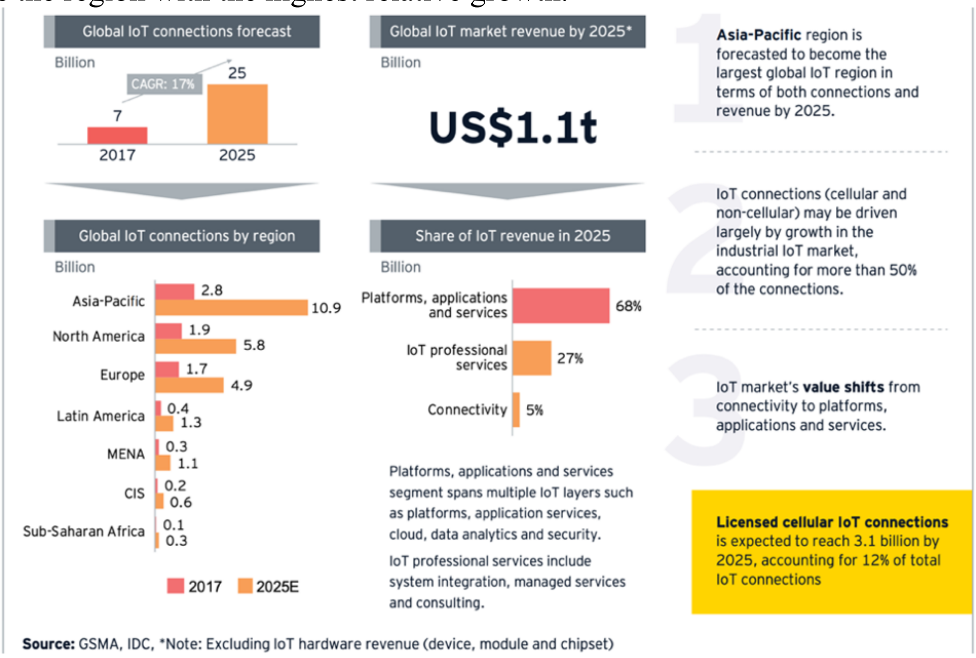

Figure 9. Market value forecast by region (FICCI & EY, 2019)

The intersection of IoT and Edge Computing brings different potential opportunities across verticals. In order to prioritize the most promising verticals for Europe, this paper evaluates the estimated global impact according to present use cases, together with Europe's competitiveness and input from the community. From this analysis, the salient verticals where Edge and IoT have the most impact for Europe are **Manufacturing, Automotive & Smart Mobility, Smart Cities and Communities, Smart Health, Smart Energy, and Agrifood & Smart Farming**.

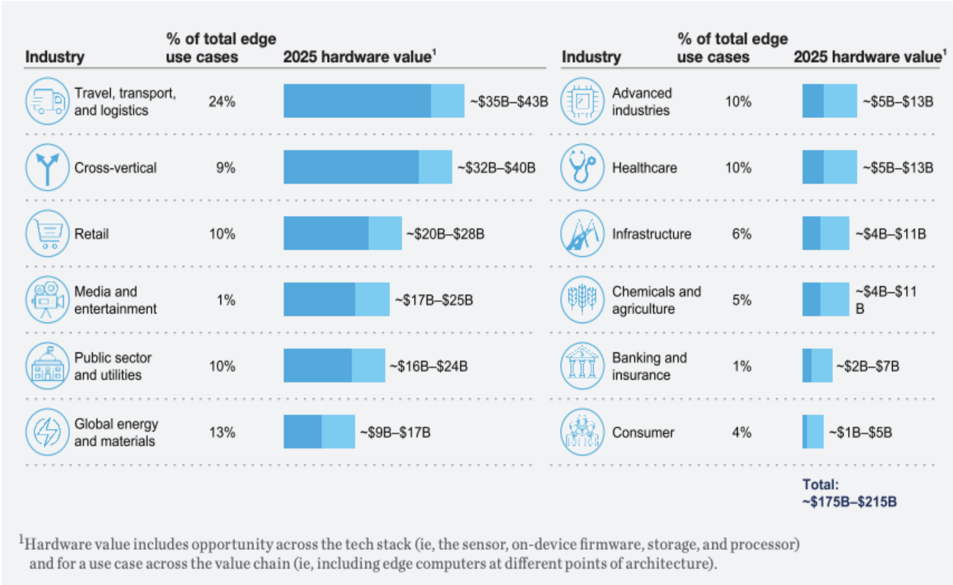

Figure 10. Market value forecast per domain (McKinsey&Company, 2018)

Despite the differences in the projections andmethodologies, two important insights can be noted: the most important domains for IoT are similar across every study, the number of connected devices is growing rapidly across all the studying domains.

Because of the types of edge computing and the slight differences in the definitions, some of the market analyses report that more than 60% of the companies in Europe use Edge to a certain extent (i-scoop, 2021). It is interesting to note, however, that in a Deloitte study with over 2000 executives (Deloitte, 2020) only 6% signalled Edge Computing as an impactful technology, whereas 64% said Cloud infrastructure would have a profound impact. IDC's European report states that European companies are lagging 2 years behind the U.S. companies who lead the edge computing development (IDC, 2019).

IDC estimates that although Edge is a marginal part of IoT infrastructure spending, it will grow rapidly, to reach 25% of total spending by 2022, with big manufacturing and automotive companies leading the way. The Electronic Components and Systems (ECS) agenda created by AENEAS, Artemis-IA and EPoSS puts the development of AI at the edge for IoT solutions on the spot, as a strategic opportunity for Europe thanks to its alignment with Europe's requirements of safety and privacy, and its expertise in embedded systems (AENEAS, ARTEMIS-IA & EPoSS, 2020). Amongst the upcoming initiatives, the Edge Computing Consortium Europe (ECCE) stands out, with over 18 companies cooperating to specify a reference architecture, develop reference technology stacks, identify best gaps and recommend best practices (EETimes, 2019).

In terms of landscape, Ericsson defines a value stack for Edge where companies addressed each of the layers, including Services, App Development, App deployment and enablement, Software, Hardware, Connectivity and Site (Ericsson, 2020). Within these layers, 4 main types of companies stand out: Hyperscale cloud providers (AWS, Microsoft Azure, Google and Alicloud), System Integrators (JR Automation, Wood, etc. (Control engineering, 2020)), Operations Technology (Siemens, Bosch, Schneider Electric, etc.) and Technology Vendors in each layer individually (Software, Hardware, Services). Although these 4 categories present similarities, their focus varies from company to company. However, a trend of lock-in strategy can be observer amongst the hyperscale cloud providers, who leverage on their cloud solutions to provide an end-to-end solution, integrating all the layers[24].

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

[24] STL Partners. AWS, Azure & Google at the edge: How much 30 fit is telco edge computing? (2017)

4 EUROPEAN LANDSCAPE - ECOSYSTEM AROUND IOT-EDGE RESEARCH, INNOVATION AND DEPLOYMENT

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

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

4.1 European Macro-environmental Context

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

It is also important to point out Europe’s leading position in smart cities and communities, acknowledging the success of the Large-Scale Pilots (LSP) programme in IoT under Horizon 2020. IoT has also a key role in the work programme part of the Multifinancial Framework 2021-2027 and related to technology development and adoption: Horizon Europe (€80 billion) (Research & Innovation) and Digital Europe Program (€9.2 billion) and Connecting Europe Facility 2 (€3 billion) (Deployment).

4.1.1 European competitiveness

With the pressing insights from the global landscape, it is now important to understand where Europe stands in the different domains cited before and how these domains will be influenced by IoT. For that matter, the matrix of Kearney in Figure 11 (AT Kearney, 2016) shows a picture of Europe and where it stands in comparison to other regions. This matrix also points to the most influenced industries, making the upper quadrants the industries of focus. The upper right corner shows the industries Europe should prioritize to remain competitive. The upper left corner shows areas where a new strategy can create big opportunities for Europe.

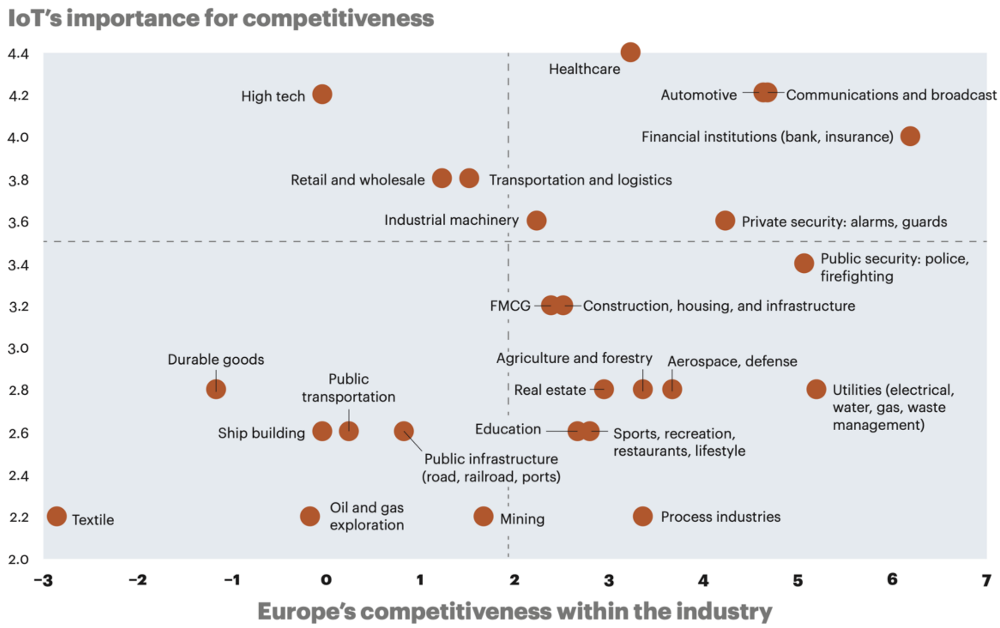

Figure 11. European competitiveness vs. IoT importance (AT Kearney, 2016)

4.1.2 IoT Value Chain to Value Network

Europe has the stakeholders to cover the various roles in the value chain: the technologies, business models, managerial skills and operational rules to create IoT solutions and go into a global market. Due to its nature, which allows the use and re-use of data, the IoT value chain becomes non-linear and it is difficult to represent it in a single dimension. To understand how value is created in an IoT context, Figure 12 shows a simplified IoT value chain. This diagram reflects the overarching nature of IoT and how it can be applied in the different industry domains. It also helps understanding the role that technology enablers play by influencing the different links (e.g. Edge/Cloud computing in the Connectivity link).

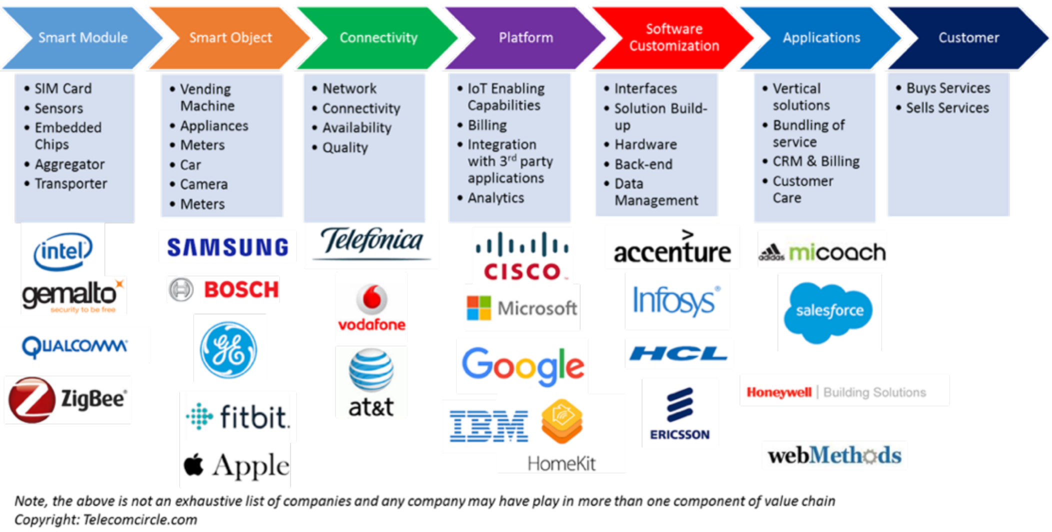

Figure 12. IoT Value Chain[25]

This section provides a picture of the basic IoT ecosystem mapping the IoT landscape – stakeholders in (e.g. standardisation provider, service providers, marketplace providers etc.) as well as the incentives, tools and money flow between the stakeholders.

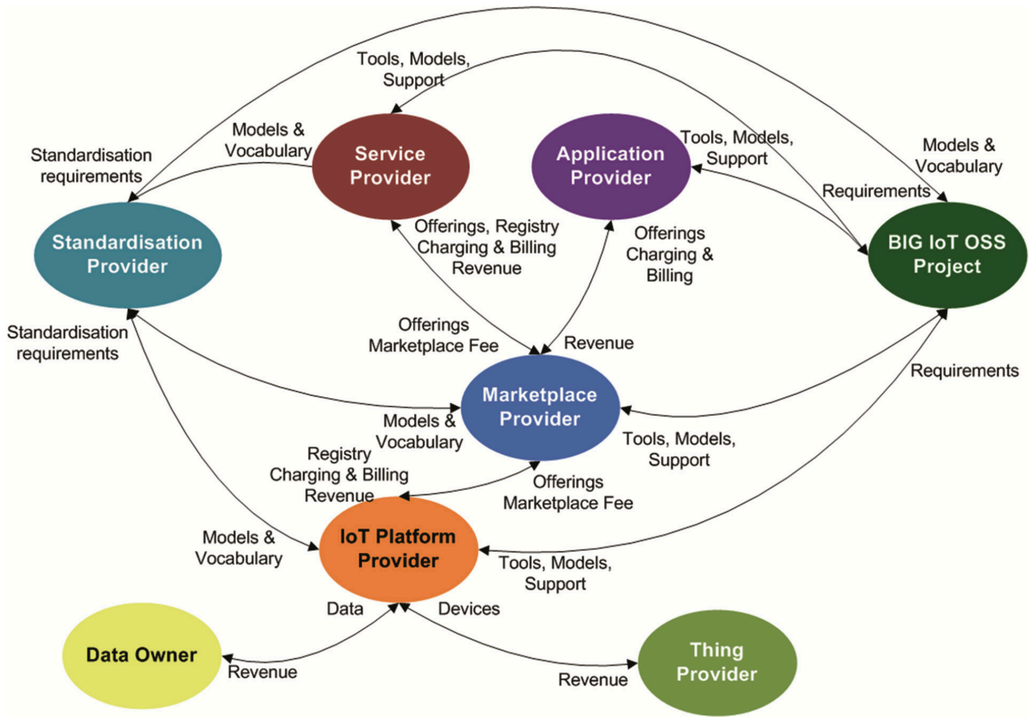

Figure 13. Value network model for Interoperable IoT systems (Schladofsky, et al., 2017)

The landscape is and will stay fragmented and, thus, European actors should join forces and collaborate to realise the potential the seismic shift offers. Opportunities are currently mostly linked to industrial IoT, and smaller entities can gain advantage by positioning themselves where there are strong ecosystems, but a different approach to the traditional value chains is needed, as the linear way of seeing the chain is not enough anymore. As mentioned, above, Innovative SMEs can enter the market through open platforms and through investing schemes.

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

Large industry players should reach out to SMEs, which often are innovative, to establish collaborations between them and with their typical competitors, under agreements like open-source developments, to allow for greater innovations and new ways of value creation to happen

4.1.3 IoT - Edge Map of stakeholders

Even though mapping the different stakeholders in the IoT/Edge ecosystem is a hard task to achieve, perhaps the one way to achieve a more comprehensive mappingis to consider both the big player/small player maps of IoT companies in the global market, the first one from IDC and the latter from IoT Analytics as shown in Figure 14 and Figure 15.

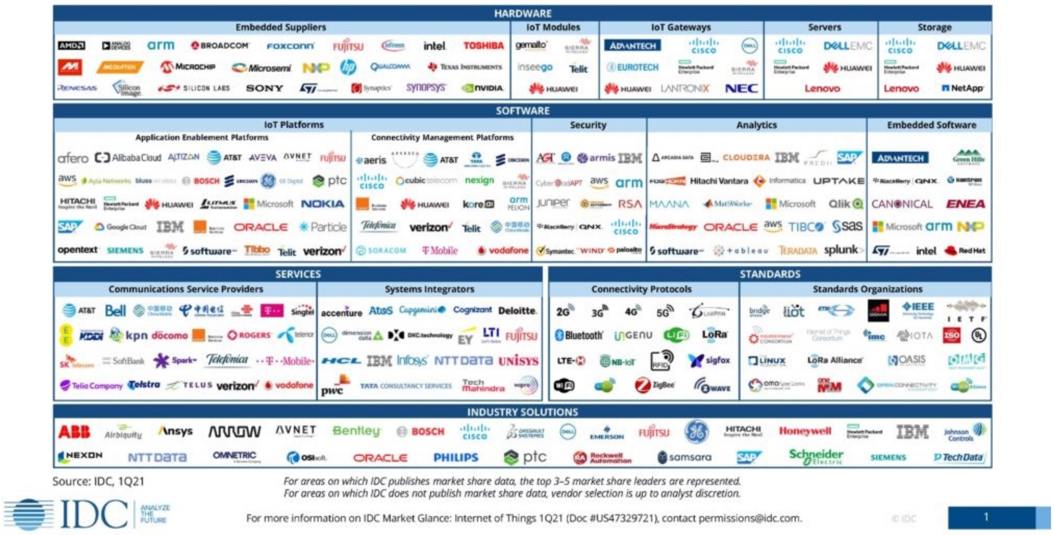

Figure 14. IoT Big Players Landscape[26]

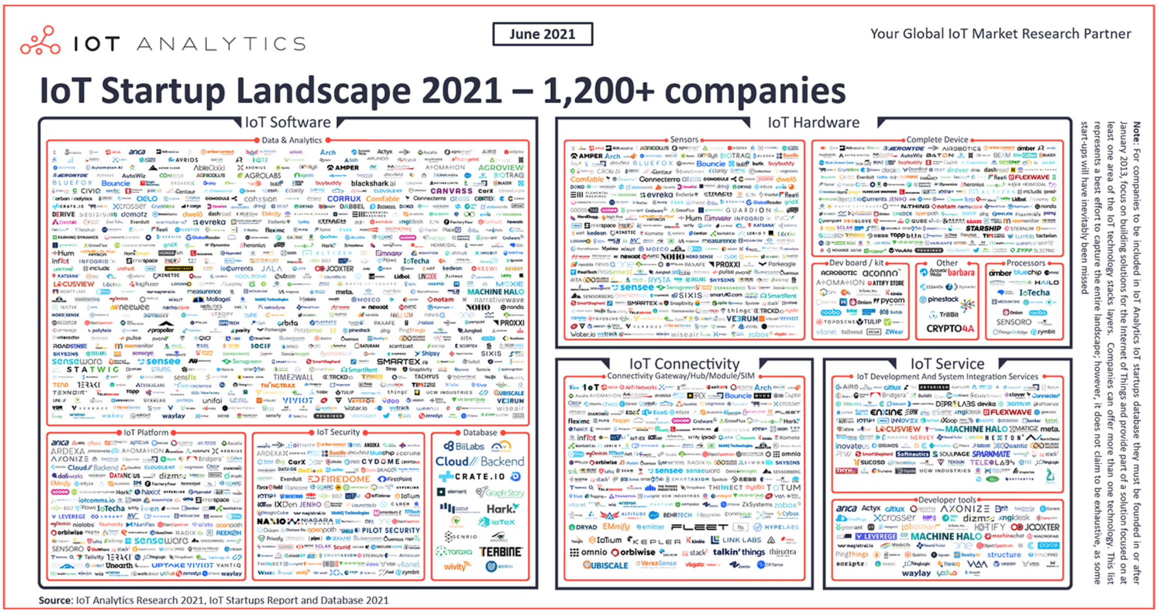

Figure 15. IoT Startup Landscape[27]

[26] https://blogs.idc.com/2021/02/08/the-internet-of-things-market-at-a-glance/

[27] https://iot-analytics.com/product/iot-startups-report-and-database-2021/

As for the more specific European Market, the report from CRISP research offers an understanding of the strongest names, specially over the DACH region in the IoT/Edge sectors, as seen in .

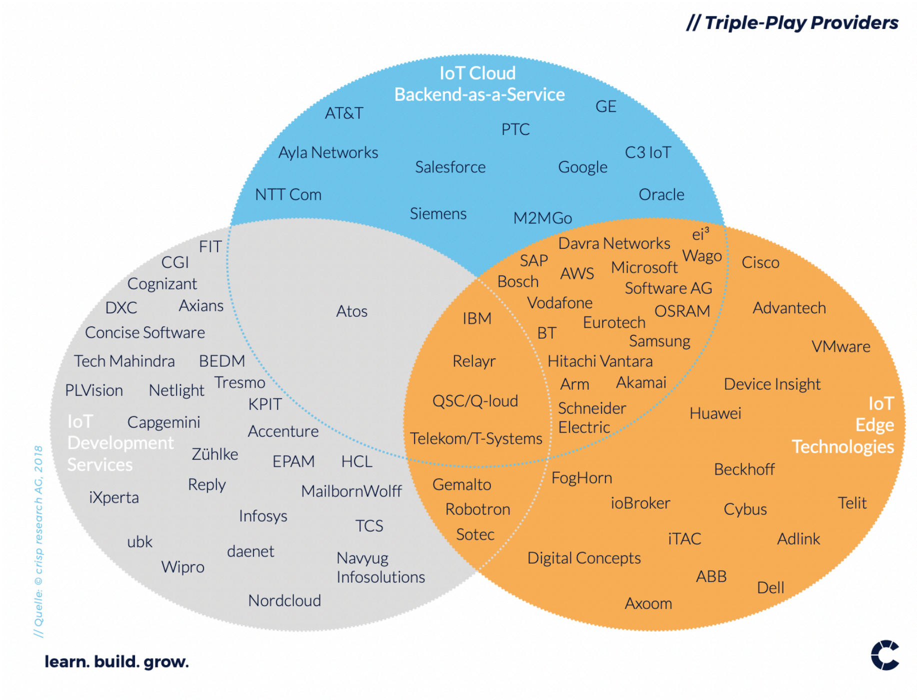

Figure 16. IoT/Edge blurring lines[28]

[28] https://www.reply.com/Documents/Report_CVU_IoT_licensed_for_Reply.pdf

4.2 Context by industry domains

The following industry analyses were prioritized based on Figure 11, the Scoping Paper, the "Market analysis and business modelling report" and the series of thematic workshops. More detailed insights are reserved for Chapter 5.3.2.

4.2.1 Agrifood & Smart Farming:

Although agriculture does not rank in one of the upper quadrants in Figure 11, it remains an important vertical for IoT in Europe. From the LSP IoF2020, Europe has fostered the creation of a symbiotic ecosystem to bring together the supply and demand sides of IoT technologies and the Agri-food sector (IoF, 2020), making it the first industrial sector to create a framework focused on data sharing (AIOTI, 2020). This framework, based on an EU code of conduct on agricultural data sharing, helps generate trust and the necessary tools to create a competitive advantage at a regional level. Furthermore, the European Agricultural Machinery Association rolled out its strategy, establishing some guidelines and best practices in the industry (CEMA, 2020).

4.2.2 Smart Cities & Communities:

Cities are the centers of next generation deployments, driven by economic and return on investment logics, as well as the search for sustainable solutions. Europe is one of the leaders in terms of smart cities and communities, with over 12 of the top 25 cities of the IESE cities in motion index (IESE, 2018). This leading position responds to Europe's early efforts to overcome the challenges of developing smart cities and communities through several initiatives aligned with the Europe 2020 targets. By promoting policies and programmes aimed at developing smart cities & communities in a coordinated way (European Parliament, 2014) and solving funding needs by Private Public Partnerships (Osborne Clark, 2015), the EU has managed to quickly develop their "Lighthouse" cities and aims to have over 300 smart cities by 2020 (Taylor, 2018). Despite the target seems to not have been reached in the context of the Lighthouse initiative, today, Europe counts with various programs constantly reinforcing its Smart City development, from the success of the SynchroniCity LSP project (European Commission, 2021) to the centralization and clusters of European Innovation Partnership on Smart Cities and Communities (EIP-SCC)[29].

4.2.3 Smart Health:

Europe faces the trend of ageing population more than ever (LSP - CREATE IoT, 2019). Although the region keeps a strong position in this industry, not all the different players are embracing change. For this industry this is crucial, since, as shown in Figure 17, Healthcare is an industry where IoT is vital for competitiveness. As one of the clusters of global challenges and European industrial competitiveness, healthcare is a top priority, with areas of intervention going from tools, technologies and digital solutions, to personalised medicine and medical systems improvements (European Commission, 2019).

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

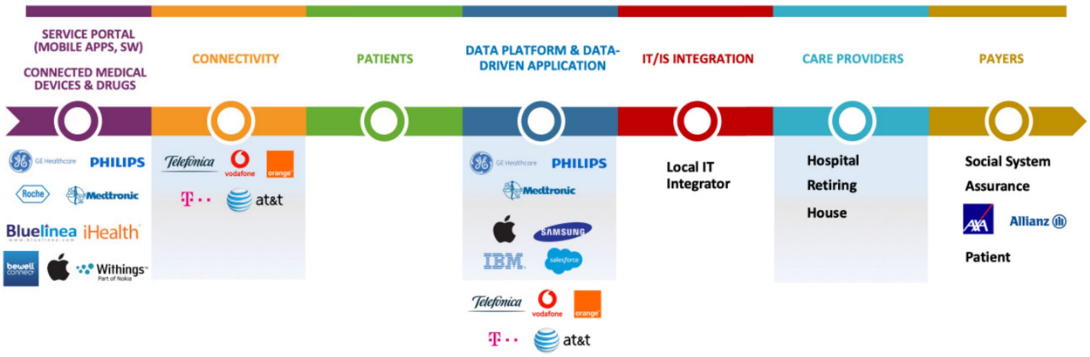

Figure 17. Healthcare Solutions Value Chain

4.2.4 Energy Management:

By 2022, it is estimated that Europeans will be able to self-generate and store power at about the same cost as when they purchase it from providers (Mobidev, 2018). The technology development in the energy sector is creating a worldwide paradigm shift where consumers become small producers. Although this brings many opportunities, it also brings challenges. A study from Deloitte mentions the main challenges to be: the production of close to one third of direct CO2 emissions, the ageing of coal and thermal plants which are still the backbone in many EU countries, the first generation wind plants reaching its operational lifetime, and the high variability of solar and wind systems (Schlaak & Truby, 2021).

The Paris Agreement, together with the European Green Deal also play a vital role in the present context, rising the regulatory pressures for renewable energy and carbon reduction. Summed to this complexity, the different projections of energy needs vary widely, with scenarios for the electricity demand ranging from 10% to 75% in the next three decades

Overall, the uncertainty of the energy transition makes it possible for many scenarios to occur. Wind and solar PV are taking the lead as coal disappears from the European power landscape, either via policy mandates, ageing infrastructure or lack of financial viability. Natural gas price volatility make it difficult to depend on as a coal substitute. Electric vehicles become mainstream in Europe. Renewable hydrogen is promising, but its deployment cannot be granted unless there is a clear climate commitment and support that helps to tilt the economic calculation in its favour vis-à-vis other options (Schlaak & Truby, 2021). Electricity trading faces growing price volatility depending on the natural sources and accurate weather forecasts are now more important than ever.

The main takeaway is that for Europe, there is no silver bullet solution for the energy transition. Different pathways, in terms of the macroeconomic environment, societal mindset and technology, can spur deep decarbonisation.

4.2.5 Manufacturing:

Having invested at higher levels than their competitors in other regions, Europe leads the way in Industrial IoT, moving to scale faster with three times more implementations than in the US (Bain & Company, 2018). Looking at individual countries, Germany paves the way with the automotive and manufacturing sectors leading the adoption rate, driven by mid-market companies (CBI, 2021). In Gartner's study (Gartner, 2019), Software AG outstands as a visionary IoT platform headquartered in Germany. Followed by the UK, France, Italy and the Nordic and Eastern European markets, the trend is passing from leveraging Industrial IoT to developing new services, to generating efficiencies and ensure cost savings. Across Europe, IoT related activities and strategic alliances are implemented, like ADAMOS, to accelerate the development (Earls, 2019). Although Europe leads the way in this domain, security, privacy and issues of trust remain important points as they hinder widespread adoption. Bain also estimates that mastering these areas will give European IoT providers a substantial competitive advantage[Error! Bookmark not defined.]. Another important challenge for this domain lies on the high-tech industry side, where several studies from Kearney show that Europe's high-tech industry declined (Kearney, 2015). Europe is struggling to keep up with the rhythm of Asia and North America. The world's biggest technology companies, like Amazon, Google, Baidu and Tencent, are all originated outside of Europe.

4.2.6 Automotive & Transportation:

With its strong mobility industry, Europe stands as an important voice when it comes to smart transportation. Starting with solutions like Asset & Fleet management and Freight monitoring in the ground transportation sectors, to Airport optimization and Passenger traffic flow, the transportation sector is an area where Europe is leading the way (IDC, 2014). In the Transport sharing area, Europe also stands out across different cities. Lastly, many European cities have already integrated smart solutions in their public transportation systems, significantly improving the quality of this service.

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

In line with the Digital Single Market Strategy[30] and its pillar 'maximising the growth potential of digital economy', the European Commission launched the Digitising European Industry (DEI) initiative[31] 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'.[32] The Internet of Things is a technology enabler that is central to the successful implementation of the EU Digital Single Market Strategy. Similarly to cloud computing, big data, artificial intelligence, robotics, machine learning, IoT will contribute to profoundly transforming the EU's economy and society.

Even though the Internet offers enormous opportunities for our society, it also brings along significant risks for our society. To address the risks while creating better opportunities, Europe aims to re-invent the next generation of the Internet by 'shaping a value-centric, human and inclusive Internet for all.'[33]

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[34].

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),

---

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

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

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

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

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

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[35].

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

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

To facilitate and accelerate the uptake of IoT across all economic sectors, the EU strategy for IoT is articulated around three pillars: a thriving IoT ecosystem, a human-centred IoT approach and a single market for IoT. A significant breakthrough was made in March 2015 when the European Commission together with IoT industry players set up the Alliance for the Internet of Things (AIOTI) to coordinate ongoing activities and build a consensus on how to unleash the full potential of IoT in Europe. In 2016, the IoT-European Platforms Initiative was formed to promote the idea of open and easily accessible platforms and to build a vibrant and sustainable IoT-ecosystem in Europe.

Given the strategic importance of IoT, a dedicated Focus Area was introduced into the Horizon 2020 ICT Work Programme for 2016-2017 and major efforts have been undertaken 'to enable the emergence of IoT ecosystems supported by open technologies and platforms.'[36]

In the same year, the IoT Large-Scale Pilots (LSPs) Programme[37] 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[38] 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[39], digital

---

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

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

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

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

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

technologies and the global race for technological R&I leadership will play a pivotal role in ensuring Europe's strategic autonomy.

Moreover, further concrete steps have been taken to translate the EU NGI Vision into key EU documents: for instance, the Horizon 2020 ICT Work Programme 2018-2020[40] 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.'[41]

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

4.3.1 The new policy context

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

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

In line with the above political guidelines, EC is defining and releasing a whole new set of strategies. On 19th February 2020 Ursula von der Leyen announced[42]:

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

---

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

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

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

Shaping Europe's digital future[43], provides the overall strategic plan to implement through different actions the "Europe fit for the digital age" political guideline. This strategy pushes three key objectives to promote technological solutions that will help Europe pursue its own way towards a digital transformation that works for the benefit of people and respects our fundamental values:

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

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

- **A European strategy for data**[44] through which the "EU can become a leading role model for a society empowered by data to make better decisions – in business and the public sector". To this aim, the strategy pushes the creation of a single market for data within Europe supported by a ***High Impact Project on European data spaces and federated cloud infrastructures***.
- **An Industrial Strategy package** focusing on EU industry transition toward climate neutrality and digital leadership as way to promote EU global leadership. The package includes different documents, most relevant ones for cloud and digital services are:
  - **A new Industrial Strategy for Europe**[45]: setting the lines for an industrial strategy aligned with core European societal and market values, including the investments on sustainable digital infrastructure needed to ensure EU digital sovereignty.
  - **An SME Strategy for a sustainable and digital Europe**[46]: focusing on concrete actions to support SMEs (as the heart of EU industry) toward a sustainable digital transition.
- **A White Paper on Artificial Intelligence**[47], promoting a European approach to artificial intelligence putting upfront key European values such as excellence and trust.
- A new set of policies[48] to ensure the sustainability of the EU economy linked to the **Green Deal**. In these landscape, one of the key goal is to "make data centres and ICT infrastructures climate-neutral by 2030".
- **A new agenda for the European strategic autonomy**[49] that encompasses the changes brought by the digital technologies and underlines the need for Europe to support its capacity to act independently and defend its sovereignty in the Digital Age;
- **The Data Governance Act**[50] promote, regulate, and enforce the data-sharing mechanisms across the EU with a strong focus on trust and security.

---

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

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

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

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

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

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

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

[50] EC. European data governance (Data Governance Act). 2020

- The **new Cybersecurity Strategy**[51] which aims at protecting Europe from "cyber threats and to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools".
- The **Digital Services Act**[52] regulates the behaviour of players in the field of online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms
- The **Digital Markets Act**[53] includes rules that govern gatekeeper online platforms. Some of these services are also covered in the Digital Services Act, however more emphasis is given in the Digital Market Act to those "digital platforms with a systemic role in the internal market that function as bottlenecks between businesses and consumers for important digital services".

Figure 18. EC strategies release timeline and relevance to Internet Things

As a follow up, in September 2020 the EC President von der Leyen, during the State of the Union Address[54], announced the preparation of a common European strategy to ensure digital sovereignty in EU by 2030. This initiative concretized in March 2021 with the launch of a Digital Compass[55] to indicate the EU 2030 strategic objectives and the relative KPIs to monitor the progresses towards these goals:

- Digital capacities in infrastructures and education & skills.
- Digital transformation of business and public services.

The digital compass finds it roots in the set of (digital) policy reforms mentioned above.

Within the Digital Single Market Strategy, the Internet of Things (IoT) represents the next step of disruptive digital innovation where 'any physical and virtual object can be connected to other

[51] EC. New EU Cybersecurity Strategy. 2020

[52] EC, The Digital Services Act: ensuring a safe and accountable online environment, 2020

[53] EC. Proposal for a Regulation on Digital markets act. 2020

[54] EC. State of the Union Address by President von der Leyen. 2020

[55] EC. 2030 Digital Compass: the European way for the Digital Decade. 2021

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

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

4.3.2 Sector specific policies

Being digitalization a key enabler for different industrial sector, EC covers it not only in Digital strategy and generic industrial policies, but as well in sector specific policies.

Following the ambitious vision of the Green Deal, EC released the Farm to Fork Strategy[56] with the aim of transitioning the food value chain in Europe toward more fair, healthy and environmentally-friendly solutions. The strategy clearly highlight the role of digitalisation in supporting this transition, from broadband connectivity to data services. In particular, the importance of data sharing, data transparency, and fair access to data is seen as essential, reinforcing the need for a common European agriculture data space, as defined in the EU Data Strategy, to enhance the competitive sustainability of EU agriculture through the processing and analysis of production, land use, environmental and other data, allowing precise and tailored application of production approaches at farm level and the monitoring of performance of the sector, as well as supporting the carbon farming initiative. The strategy also highlights how agrifood digitalisation should be accompanied by proper investments on up skilling workers in the sector.

Also the transport sector policies evolved in light of the Green Deal goals. The Sustainable and Smart Mobility Strategy[57] sets a plan for the 90% reduction in the transport sector's emissions by 2050. To achieve this goal, the EC promotes the wide adoption of digital technologies, from 5G to artificial intelligence, and from edge computing to autonomous drones. The strategy clearly identify that, for the digital transformation to happen in the sector, more efforts toward fair and trustworthy data access, share and exchange are required. Accordingly regulatory actions are foreseen to facilitate the establishment of the Mobility Data Space as envisioned in the EU Data Strategy. Specific actions are envisioned to guarantee fair and effective access to vehicle data by mobility service providers.

To accelerate the green transition in the Energy sector, EC released the Clean energy for all Europeans[58] package that orchestrate the overall strategy to target climate neutrality for the

---

[56] EC, Farm to Fork Strategy, 2020

[57] EC, Sustainable and Smart Mobility Strategy, 2020

[58] EC, Clean energy for all Europeans, 2019

energy sector in Europe by 2050. While this plan only briefly the role of digitalisation in the sector, the linked policy EU Strategy for Energy System Integration[59] discusses the importance of digitalisation to pave the way towards an effective, affordable and deep decarbonisation of the European economy. Several digital technologies are covered in the strategy, including big data, Artificial Intelligence, 5G and distributed ledger technologies. A key role is played by cybersecurity given the vital role of energy infrastructures, and to secured and trusted data exchange with the ultimate goal of establishing a Common European energy data space as announced in the European Data strategy. The strategy includes as the role out of smart metering and measures to ensure the interoperability of energy-related data.

The new action plan for circular economy[60] position digital technologies, including internet of things, big data, blockchain and artificial intelligence, as key enablers for the creation of an EU wide ecosystem of circular economy, from the role of digitalisation of product information to enable their traceability along the value chain, to the importance of enabling data exchange across the actors belonging to different value chains to enable a cross sector circular economy.

4.3.3 European programmes for research, innovation, deployments and infrastructures

As part of the MFF 2021-2027, the European Commission launched three programmes acting as key pillars to support the digital transformation in Europe:

- Horizon Europe, the research and innovation programme with a € 95.5 billion budget, including € 15.3 billion on the 'Digital, Industry and Space' cluster.
- Digital Europe, a new programme focusing on building the strategic digital capacities of the EU and on facilitating the wide deployment of digital technologies, with a € 7.5 billion budget.
- Connecting Europe Facility 2, focusing on the creation of transnational digital infrastructures with a € 2.07 billion budget out of the total CEF budget of €33.71 billion

These three programmes are meant to complement each other and play a key role in Europe's digital transformation in connection with the Internet of Things technologies. While Horizon Europe provides future outlook by supporting cutting edge research and innovation, Digital Europe and Connecting Europe Facility will foster the market deployment of mature technologies (including those that proved maturity and business viability from Horizon 2020 and, in the future, Horizon Europe). The introduction of the Digital Europe Programme may play a key role in supporting the deployment of mature research and innovation outcomes, bridging them between the Research and Market penetration phases, thus helping to overcome the so-called "Valley of Death".

[59] EC, Powering a climate-neutral economy: An EU Strategy for Energy System Integration (COM/2020/299), 2020

[60] EC, Circular Economy Action Plan, 2020

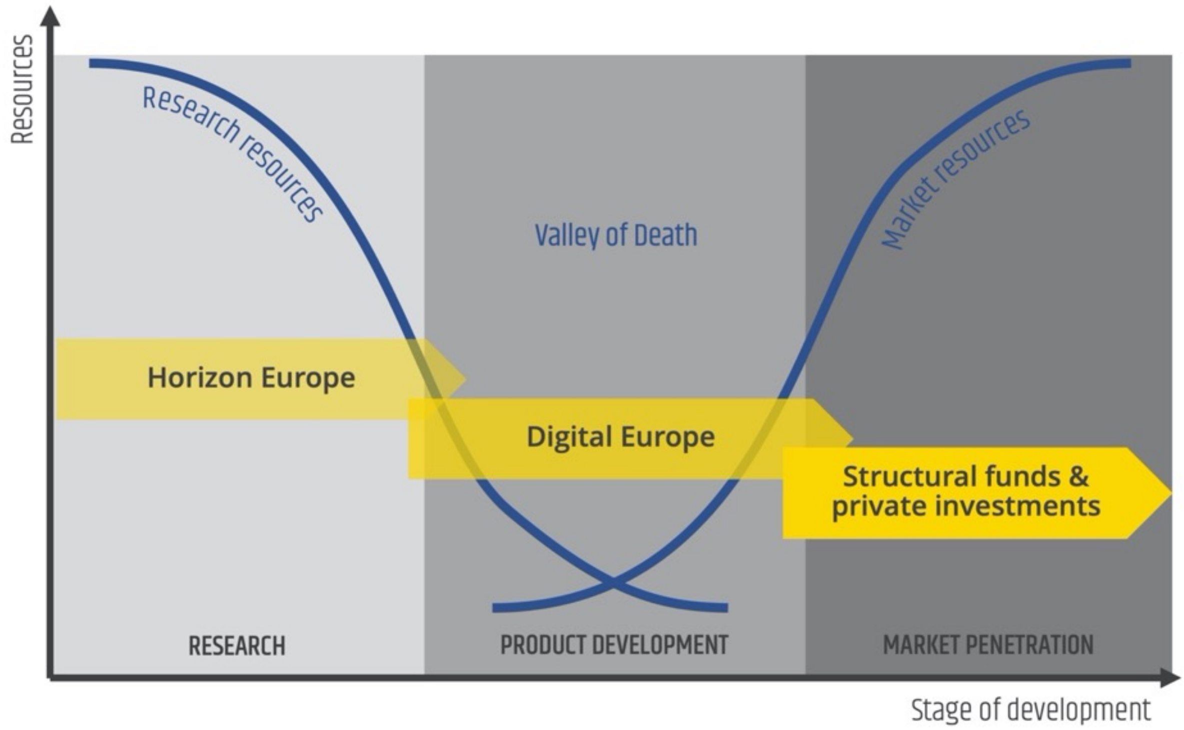

Figure 19. From research to market: the role of EU instruments.

4.4 General Ecosystem

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

- **Initiatives.** In the current European landscape, several initiatives drive IoT or support its development. Primary actors in the driving ecosystem include AIOTI and IoT Forum. Other actors focus on linked technologies, these include for example: NGI focusing on human centric internet, 5G-IA[61] focusing on next generation mobile networks and services and BDVA focusing on data-centric technologies to generate value from data insights. Other initiatives again focus on specific application area, such as: OASC[62] focusing on reference solution for smart cities and communities and ARTEMIS (now INSIDE)[63] focusing on embedded intelligent systems industry.
- **Industries.** The European industrial ecosystem linked to IoT in Europe is quite wide, spanning from embedded device developers, network operators, system integrators, platform providers and vertical solution providers. Several of these players have a clear (and public) vision of the role of IoT and related technologies into shaping our future society. ATOS in its "Look Out 2020+ Tech Trends" (ATOS, 2021) classify Internet of Things together with Deep Learning, Digital Twin and Autonomous Vehicles as Transformation technologies. SAP in its "Innovation Guide" (SAP, 2021) identifies a number of key scenarios where IoT, in combination with other technologies, will revolutionate the market or - in some cases – it is already transforming it. More detailed information was described in section 4.1.3
- **R&I projects.** In the past few years a number of projects have been active in relation to IoT as part of the Internet of Things unit or other units part of DG Connect. In the recent past, the LSP (Large Scale Pilot) projects and IoT-EPI (IoT-European Platforms Initiative) projects collected the most relevant projects aiming at developing and piloting IoT technologies. In 2019 a new set of Pilots have been kicked off as part of the Digital Platform cluster of projects part of the Technologies and Systems for Digitising Industry unit.
- **SDOs.** Standard Development Organisations are one of the primary actors in the establishment of IoT interoperable solutions. The future IoT market will be framed by global standards developed in international SDOs and not by regional standards. While the European research and innovation programme has been efficient in supporting regional Standard Development Organisations (SDOs) such as ETSI and CENELEC, global SDOs & Industry Associations such as IEEE, IETF, ITU, ISO, IEC and TM Forum are priority stakeholders in the European standardisation landscape.
- **Open Source communities.** IoT since its infance have been linked with Open Source. Nowadays a number of mature projects, spanning from hardware to platform and

61 https://5g-ia.eu/

62 https://oascities.org/

63 https://artemis-ia.eu/

scenario specific solutions are getting mature. Some of these communities, such as Arduino[64] for the hardware, and FIWARE[65] for the platforms, have deep European roots.

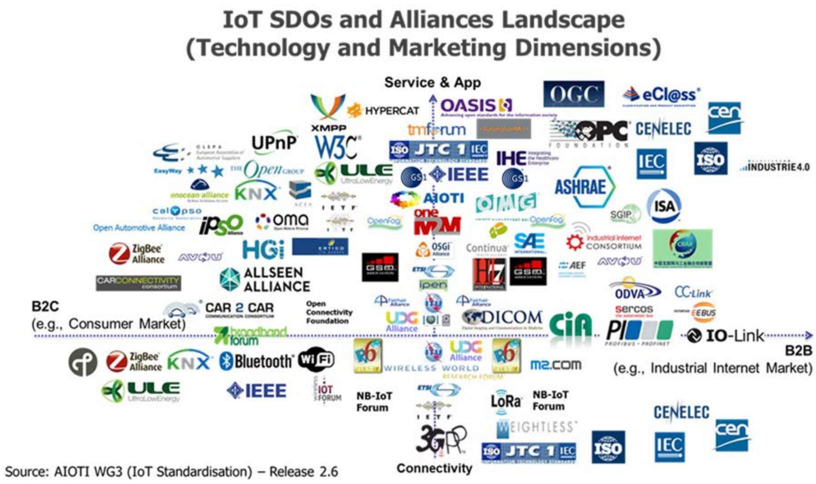

Figure 20. IoT SDOs and Alliances Landspace (source AIOTI WG3)

Figure 21. IoT-Edge European Ecosystem Draft

64 https://www.arduino.cc/

65 http://fiware.org/

4.5 Privacy and Security Ecosystem

Through its privacy, security and trust observatory and together with the European IoT Security and Privacy, NGIOT has mapped relevant initiatives and tools in this context of the IoT ecosystem.

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

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

As regards IoT security, experts observed that the new data paradigm where less data will be stored in data centres, and more data will be spread in a pervasive way closer to the user 'at the edge', brings new challenges for cybersecurity. It was also observed that, securing IoT applications is not just about protecting personal data and and business data, it is about protecting people as individuals, as citizens, and as users of services. Three major areas of large innovation potential are: secure elements; cryptography and Blockchain[66].

The following table summarizes the webinars that have been organised and hosted by NGIoT in order to map the initiatives in the IoT European communities that were useful to gather information to analyse the actual framework of research and pool together all the relevant best practice identified by the abovementioned community.

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

Webinar	Date
Data Protection in the transport field: IoT,IoV and Crime Prevention	25.02.2020
EuropeanCommission Data Strategy	13.03.2020
The EC White Paper on AI	03.04.2020
Integrating privacy in the IoT ecosystem	10.04.2020
Safety and liability implications of AI, IoT and robotics	24.04.2020
The work of the ETSI Task Force 547 on Security, Privacy and Interoperability of standardisedIoT Platforms	08.05.2020
DevOps for trustworthy IoT systems	15.05.2020
The interoperability in IoT platforms: the SOFIE framework	05.06.2020
Physical Audience Measuring Technologies and Privacy concerns	26.06.2020
NGIoT Webinar: Going Public – providing access to our IoT innovations	03.07.2020
5G and IoT	10.07.2020
Open webinar on the impacts of the EU Court of Justice ruling "Schrems II".	24.07.2020
Global Reflections on the EU Approach to AI and Data Governance	28.07.2020

Table 1. Webinars organized by the NGIoT Observatory in the context of NGIoT WP2 activities

Having mapped all the relevant initiatives, with the involvement of SMEs and stakeholders in the field of the industry and research, it is possible to set up guidelines for the enhancement of trust in end-users through a data protection and cybersecurity compliance path for IoT.

The protection of personal data, cybersecurity and, ultimately, an ethical and human-centred approach to the use of the IoT, leads to a growth in trust in the use of devices and a greater involvement of end-users that could lead to an increase in market potential.

In this sense, the evolution of technology should lead the legislator and the Commission to the creation of focus groups and projects dedicated to understanding how to instantiate the principles already included within the GDPR, within a legal tech approach in the design of IoT devices.

A good example of such an approach could be the identification of luminous signage on IoT devices to visually represent data flow. The activity referred to in the example is not as trivial as it might initially seem, since it is a matter of identifying a standardisation process as it was for traffic lights in the early 1900s, i.e. identifying those luminous signs that become commonly used by all sectors and that are intuitively clear to users, in such a way that personal data processing operations are immediately understood by the end user. This approach, which represents a valid synthesis and an adequate example of what the future of legal-tech research in the field of IoT will entail, is only one of the elements that allow the principles of the Regulation to be instantiated directly on devices. The legal tech design approach, oriented to the standardisation of the aforementioned instantiation, is the matrix from which to draw inspiration to further enhance the IoT adoption processes in Europe. The legal tech design approach should therefore be based on considering the best practices identified as prerequisites for industry and research in Europe, while future fields of research should include those sectors, such as device signage, that need further investigation in an effort to achieve a common approach. In this sense, in conclusion, education, digital skills, training and awareness are extrinsic to the addition of technical components privacy by design that lead the user to master and become aware of the IoT world around him, thus allowing the end-users to freely choose and dispose of their personal data, to feel cyber-secure and to provide in return useful feedback for the improvement of products in all fields, from e-health to smart communities.

4.6 Map of European initiatives

As reported in the **IoT Large Scale Pilot (LSP)** Programme eBook[67], IoT brought the Internet society to the next stage of development, with new values introduced, piloted and established, along with new IoT-oriented business models and building on a combination of connected devices, infrastructures, services, information and stakeholders as part of a consistent and integrated ecosystem. These values have been used, tested and assessed through the LSPs strengthening even more the fact that the adoption of IoT is a key step and challenge towards the 'Digitising European Industry' strategy and the Next Generation Internet of Things. In such a configuration, IoT acts as a catalyst for the digital revolution and brings transformation in several societal aspects, although, posing new challenges to the entire ecosystem. LSP projects focused on five key domains: i) Smart Living solutions for ageing people; ii) autonomous driving vehicles and releated mobility services; iii) smart food and farming solutions; iv) innovative services for cultural and heritage industry and v) Smart City services. All the projects focused on common aspects in the respective domain to deliver reference solutions that could be easily replicated across Europe. Between January 2019 and 2020 a new set of Large-Scale Pilots for Digitising European Industry started covering: Agriculture, Energy, Healthcare and Manufacturing.

The **AIOTI** Strategy 2017-2021[68] covers several key aspects related to IoT and related technologies. It highlights how new technological advancements will emerge from current R&D activities on 5G networks, Artificial Intelligence (AI), robotisation, quantum computing, blockchain and nanotechnologies uses. Such advancements will lead to new application domains with IoT-oriented concepts and solutions. The strategy also highlights that the biggest and ***most critical challenge remains the trust in IoT technologies and applications in and by society***. Such a challenge requires discussion around the involvement, education and information of the stakeholders in their context and environment. In 2019 AIOTI released "AIOTI Vision and Recommendations: European IoT challenges and opportunities 2019 – 2024" 69: a set of reccomendations for the upcoming work programmes. In particular the reccomendations highlights: the ***importance of a human-centric approach*** – as the European vision for IoT - ensuring safety, security, privacy and trust; the ***priority of closing the digital divide*** between EU regions and the Member States; the importance for EU society of the development of key ***IoT-enabled solutions addressing societal challenges like energy efficiency, climate-change, carbon-neutral smart cities, security of food supply and healthy water***; the key role - for the creation of the European digital single market - of ***cross-sectoral IoT data marketplaces***; the primary role of cyber-security strategy for safeguarding IoT technology and applications, whilst ensuring privacy by design; the ***advancement of the convergence of IoT with other enabling technologies*** such as next- generation connectivity, AI and edge computing.

Along the same line, the **Road2CPS** Technology and Application Roadmap[70], 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,***

---

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

68 https://aioti.eu/aioti-strategy-2017-2021/

69 AIOTI. European IoT challenges and opportunities 2019–2024 (2019)

70 Road2CPS. D2.4 - Strategy Roadmap (2016)

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)[71] 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[72] 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**[73] 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[74] discusses IoT among other key technologies like embedded 5G, Big Data, quantum computing, cloud, mobile and embedded systems and smart grids as the most relevant and critical towards secure ICT infrastructures. Especially for IoT adoption, the challenges and needs in the cybersecurity domain focus on ***new computational trust models***, the ***inter-connectivity of smart systems***, the ***interoperability protocols for consistent and efficient communication*** and transfer of information, and the ***trust in IoT devices and IoT frameworks***.

The **AENEAS, ARTEMIS-IA and EPoSS SRA**[75] focuses on Electronic Components & Systems. This SRA, while tackling a wide set of aspects going beyond IoT per se, provides an interesting analysis covering different industrial sectors including transport and mobility, health and well-being, manufacturing, energy and security. Starting from an analsys of challenges in the different industrial sectors, it provides as well challenges for the electronic components and system industry. The SRIA highlights the importance of advancements and adoption of the following technologies: Artificial intelligence and data analytics, Edge computing and novel computing architectures (such as Neuromorphic computing), 5G, Advanced electronics (including Bio-inspired devices and Photonics). A detailed timeframe is provided for the advancement in computing and storage technologies and in process technology for

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

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

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

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

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

manufacturing of electronic components, which are highly relevant to the IoT edge gateways, devices and sensors development.

Finally, the report provided under the **NGI Initiative**[76] 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.

[76] HUB4NGI. NGI Guide v3 (2019)

4.7 SWOT analysis from market research and community input

The following section presents the main strengths, weaknesses, opportunities, and threats identified through survey, interviews with experts from various sectors and the NGIoT Strategy Board. The scope of this SWOT analysis stays within the specific aspects related to Research, Development and Innovation in the field of IoT and Edge computing in the EU.

4.7.1 Methodological approach

The SWOT analysis is based on:

- **Stakeholders' inputs** collected through surveys, interviews, and meetings with the NGIoT Strategy Board[77]
- **The NGIoT thematic workshops**
- **The results of NGIoT WP2** on trust, security and privacy
- **The market analysis** performed in WP3 to analyse the socio-economic environment and market opportunities for the future research programme on IoT, Edge Cloud.

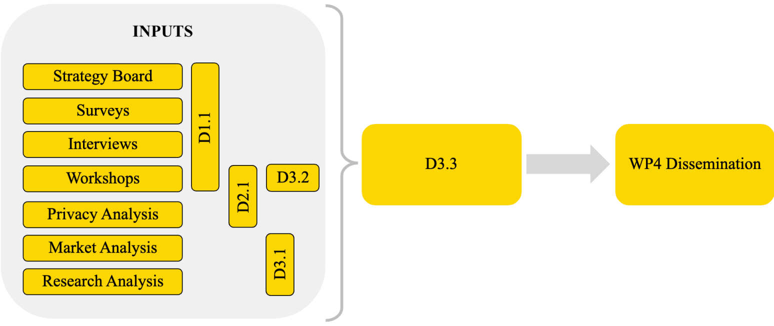

Figure 22. SWOT collaboration structure

These complementary sources have been integrated and used to generate a synthetic SWOT analysis. It was then enhanced by iterative desktop research to strengthen and challenge the insights and convergence areas and interactions with the NGIOT Strategy Board. We retained the most relevant ones and ordered them in decreasing order of importance. Finally, the SWOT was once again presented to the Strategy Board and the NGIOT consortium for the last details.

4.7.2 Strengths

Large funding and programme for research and innovation: The European research and innovation programme Horizon Europe is the largest one in the world, with over 95.5 billion euros invested with several particularities that show an evolution from the Horizon 2020 programme, focusing on open science, equality, interdisciplinary research and practical applications, while addressing pressing societal challenges like climate change, health and the digital revolution (Schirmeier, 2021). Having invested over 500 million euros on IoT research and development under the past Horizon programme (European Commision, 2021), IoT and Edge are key components of many of the new programme's goals, which represents a strength for the deployment of these technologies within Europe in the upcoming years.

Strong SMEs presence: The European econmy benefits from a strong ecosystem of SMEs that are the backbone of the European economy (European Commision, 2021). SMEs are critical for social mobility, globally accounting for 95% of new job creation while enabling people to

[77] NGIoT D1.1 IoT Ecosystem building vision and report

exit poverty and enter the middle class. Although the adoption of new technologies represents an important challenge for SMEs globally, SMEs can be highly innovative and more productive than larger companies (OECD, 2018). Nevertheless, studies find that older SMEs are more prone to get better results from their R&D than younger firms, although the main barrier for this phenomena is financing (Ferrando, Lekpek, & Veugele, 2019).

Generally well educated human resources / people & strong academic landscape: statistics from Eurostat account for 8.4 million ICT specialists in the EU as of 2020 (eurostat, 2020). Compared to the 55.3 million specialists projected worldwide (Mlitz, 2021), the EU accounts for around 15% of the global count. The EU counts with a strong tertiary education and programs focused on enhancing ICT education. A key example of this, specifically for IoT is the Project IOT-OPEN.EU which aims at improving higher education for European digital global competitiveness (iot-open.eu, 2016)

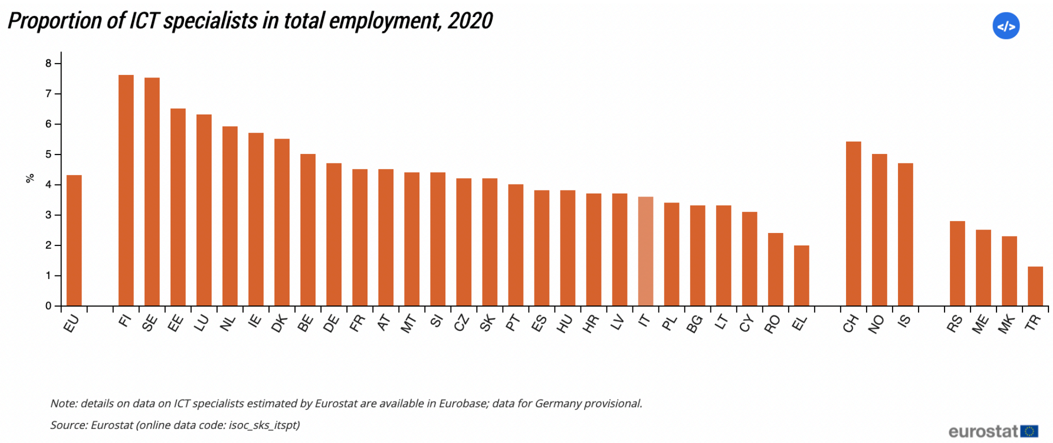

Figure 23. Proportion of ICT specialists

Collaboration between European institutions, member states and research centres: Europe can be considered the epicenter of research collaboration, with many programmes and initiatives aiming at erasing the boundaries of knowledge. Science Europe, the Joint Research Centre, just to mention some, together with the many hubs of different fields and bilateral collaboration between centres make up for a vibrant cross-border ecosystem. Specifically for IoT, initiatives like AIOTI, NGIoT, as well as projects like IoT NGIN reflect the solidity of this collaboration.

Strong manufacturing and automotive industry: Being crucial for EU's prosperity, the manufacturing and automotive industry provides over 33 million and 13.8 million jobs respectively, the latter representing 6.1% of total EU employment (European Commission , 2020). The manufacturing sector, including the automotive one, generate over 15% of the European GDP. Europe is among the world's biggest producers of motor vehicles, with this sector representing the largest private investor in research and development (R&D) within the estimated two thirds of R&D investment accounted by the private sector in the manufacturing domain (Euraxess, 2016).

Cellular coverage and communications & Top leading 5G vendors: Europe is positioned in first place when it comes to mobile broadband coverage (ITU, 2020). Although 5G rollout is perceived as slow when it comes to the implementation of the enhanced Mobile Broadband (eMBB), Europe counts with two of the three 5G leaders according to Gartner (Ericsson, 2021). Specifically for IoT research and its relationship to 5G rollout, Europe has a number of early-stage 5G networks up and running, including the first applications of mMTC with pilots use cases across focal industry verticals (European Investment Bank, 2020). Europe also counts with technology leaders developing 5G industry testbeds (5G-ACIA, 2021).

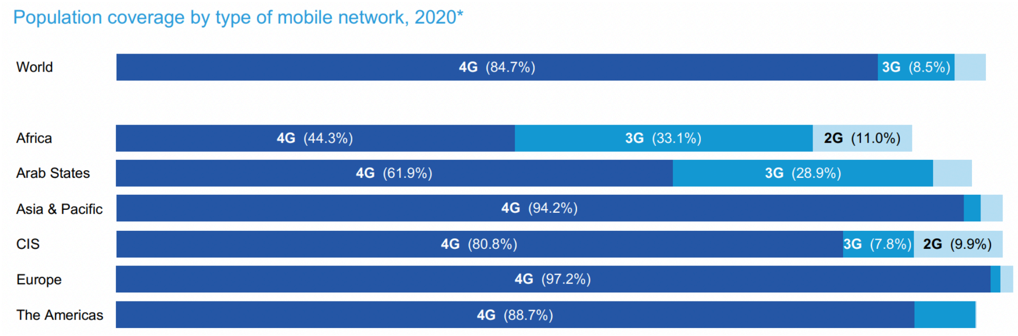

Figure 24. Mobile broadband coverage

Widespread market adoption of consumer electronics: While 60% of the global population are internet users, in Europe the rates of the subregions are 96% for the north, 93% for Western Europe, 86% in Southern Europe, and 82% in Eastern Europe to the Digital 2021 Global Overview report (European Fundraising Association, 2021). A study by Mckinsey shows that adoption jumped from 81 percent to 95 percent as a result of the COVID-19 crisis (McKinsey, 2021). This digitalisation of society lays the ground for an attractive market for IoT-Edge deployment.

Privacy and security policies and culture & Strong expertise in data protection by design approach: Many of the data processing activities involved in the operation of IoT will fall within the material scope of the General Data Protection Regulation (GDPR), making data protection a built-in requirement for any IoT solution as part of the principle of 'privacy by design' (PwC, 2016). By developing this regulation Europe is at the forefront of the privacy and security policies globally, with over 140 countries adopting regulations in line with the GDPR. This positioning sets a baseline through Article 13 to enhance the control of personal data for data subjects, which increases trust and allows for stronger for business and research development thanks to the feeling of security and control about data (NGIoT D2.1, 2021).

Active research community, mobility support & top journal publications: The ICT sector represents 4.8% of the European economy, generates 25% of total business expenditure in R&D, and investments in ICT that account for 50% of all European productivity growth (WBC-RTI, 2016). According to a report by the U.S National Science Board, while the worldwide S&E publication output continues to grow on average at nearly 4% per year; from 2008 to 2018, output grew from 1.8 million to 2.6 million articles (NSB, 2018). In 2018, China (with a share of 21%) and the United States (with a share of 17%) were the largest producers just behing the EU as a group (with a share of 24%) (NSB, 2018).

Strong expertise in public-private partnerships: From the 1990s to the 2018s, 1749 PPPs worth a total of 336 billion euro have reached financial close in the EU (European court of auditors, 2018). Although the report mentioned before signaled the shortcomings of the audited PPPs, Europe has developped strong expertise, with the institutionalization of such model through organisations like the European PPP Expertise Centre (EPEC, 2021)

Strong expertise in industrial data: The best reflection of this strength is the recent creations of the European Alliance for Industrial Data, Edge and Cloud (European Commission, 2021) and the Data Spaces Business Alliance (DSBA),as the strong industrial development history in Europe sees the need of strengthening and accelerating the data management on an online secure way. Aligned with the Data Strategy from the EC, some of the most important organisations to mention include Gaia-X European Association for Data and Cloud AISBL, the Big Data Value Association (BDVA), FIWARE Foundation, and the International Data Spaces Association (IDSA).

4.7.3 Weaknesses

Market regulatory and linguistic fragmentation: Even if over half of EU Internet use a language online that is not their native language, a study from Eurobarometer also found that 90 percent of EU Internet users prefer to use sites in their own language (DW, 2011). This fragmentation together with country-specific regulations, make big scale deployment a major challenge, although there are already initiatives in place to bring this barrier down like Language Technologies for Multilingual Europe (SRIA, 2017).

Slow time to market (research to end-result process to market): Europe struggles to bring ideas and innovation to the market. D1.1 points to VC investments as one of the possible reasons/solutions to this weakness. Even though Europe produces more scientific publications than China and the US, disruptive innovations are uncommon in the EU, there are significantly less unicorns and venture capital funds are significantly lower and concentrated in only 8 member states (NGIoT D1.1, 2021).

Missing digital skills to address the market needs: According to the 2020 Digital Economy and Society Index (DESI), 42% of Europeans do not have basic digital skills and 54% of SMEs struggle to recruit digital experts. On top of this issue, companies often find fragmented and unevenly distributed information, resources, training and funding opportunities, especially across borders. (DIGIBYTE, 2021).

Lack of fertile ecosystems for startups and European industrial leadership: Europe's start-ups are fewer in number, raise less money, and have a lower likelihood of success (which we defined as start-ups that reach Series C funding, go public, or are acquired) than those in the U.S according to a McKinsey study. (McKinsey, 2020)

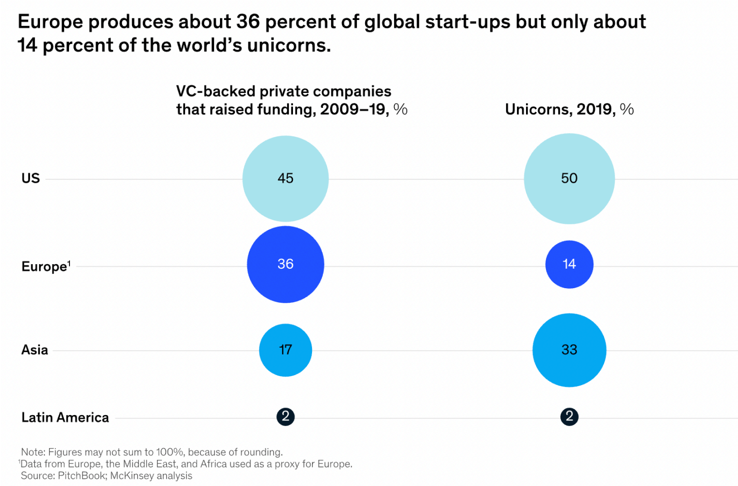

Figure 25. Global start-up ecosystem.

Bureaucratic and ineffective processes & bureaucratic culture and lack of agility: the European institutions have long been criticised for their bureaucracy and lengthy reaction time (EuChems, 2019), and even though actions are being taken to counter these critics, still the perception prevails. As an example, representatives of the Australian and New Zealand governments recently raised concerns over the "bureaucratic burden" of taking part in the EU's research and innovation programmes (Bisson, 2021).

Poor talent retention (brain drain): Brain drain has a socio-economic impact. Poor talent retention is a problem faced by many parts of Europe, and it is characterized by the migration of highly skilled laborers to other countries, especially the US, as well as mobilisation inside the EU (AER, 2020). Amogst the main identifie factors for this phenomena are attractive salaries outside Europe, short-term fixed contracts for early career researchers, unfair recruitment procedures, attractive migration policies, and the indirect role played by internationalisation policies to encourage permanent mobility (Khan, 2021)

Insufficient trust in cybersecurity and innovative technologies, resistance and fears with regards to digital transformation: In its deliverable D2.3, NGIoT signals a need for improvement in terms of data privacy, transparency and effective "*explainability*". It also points as main weaknesses in this field the end-user education, especially in terms of rights, the "*black box effect*" which is the lack of a unique centre of liability to identify who was in control of the IoT system and lack of a high risk classification.

Lack of standards, interoperability in IoT/Edge computing and adequate regulations in certain domains: Artificial Intelligence/Machine Learning, Cloud-Fog-Edge, including network virtualisation (NFV, SDN) and Cloud-native, 5G and 6G standardisation is a critical need for Europe to invest and be present in. A common framework and APIs, IoT interoperability and Security standards can facilitate development of new technical solutions.

Women in STEM still not always well regarded in some EU countries: The vast majority of persons employed as ICT specialists in the EU are men. The share of ICT employment that was accounted for by men stood at 81.5 % in 2020 with only 3 member countries with a percentage lower than 75% (eurostat, 2020).

Lack of IPR generation for building competitive advantages and raising VC investments: Europe is largely underrepresented in international patents filled at WIPO in the domain of IoT, Edge and Cloud technologies, as well as in enabling technologies such as 5G, AI, DLT, Digital Twins. Therefore, it may face issues in terms of freedom to operate and risk to depend on non-EU IPR with associated royalty costs.

IPR patenting cost very expensive compared to other regions: Patenting costs are quite high in Europe compared to other regions of the World. For instance, filling a patent in China appears to be practically free for Chinese companies.

Lagging in 5G deployments and adoption for IoT:

Although Europe is starting the commercial rollouts for standalone networks, its 23% of 5G rollout falls behing the US and the near 100% adoption in countries like South Korea . Patenting in 5g is invisible.

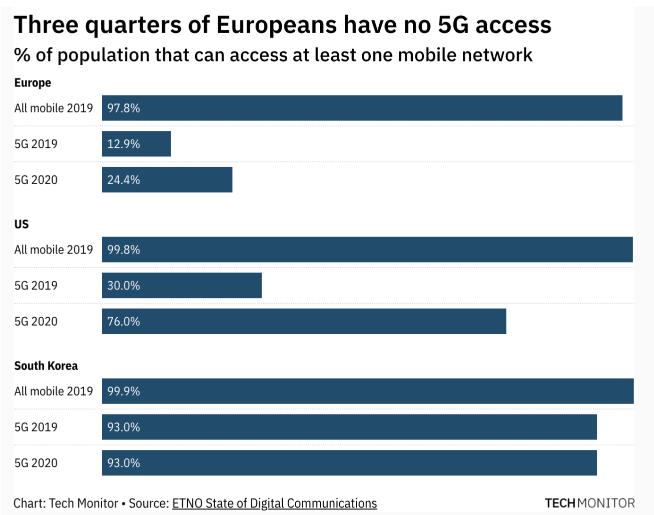

Figure 26. Access to 5G in Europe

Scarcity of European global industrial leaders: Europe depends on non-European suppliers in several domains: Cloud services, hardware manufacturing, etc. This raises the question of its technological sovereignty. This is specially true for the platform link in the value chain, the

European cloud industry is dominated by three major hyperscalers which control 70% of the IaaS market: Amazon with AWS (53%), Microsoft with Azure (9%) and Google Cloud (8%). In the meantime, european cloud specialists and telecom operators are gradually increasing their foothold with OVHcloud and Deutsche Telekom are ranked third and fourth in their respective countries (OVHCloud, 2021).

4.7.4 Opportunities

IoT market expected to be a very large and fast-growing market:

As described in section 3, both IoT and Edge Computing markets show strong growth projections for Europe across many of the verticals and driven by other technology developments.

International adoption of data protection regulations & Regulatory evolution in data protection and cybersecurity which can constitute a competitive advantage:

Following the entry into force of the GDPR, many other countries in the World have adopted similar regulations. This normative evolution is creating a new market for privacy by design technologies in the IoT, edge and cloud domain. A study from Thales finds there are more than 120 countries "engaged in some form of international privacy laws for data protection to ensure that citizens and their data are offered more rigorous protections and controls" (Thales Group, 2021), defining the global privacy landscape as "in flux", pointing to probable future alignment where Europe plays as a pioneer.

Digital transformation in all verticals & Era of digital manufacturing and industry 4.0:

Industry plays a central role in the economy of the European Union, accounting for 15% of value added (compared to 12% in the US). It serves as a key driver of research, innovation, productivity, job creation and exports. Industry generates 80% of the EU's innovations and 75% of its exports, and according to a study from Iberglobal, even if Europe's industry has lost ground in the past two decades, there is a chance that Europe will increase its dwindling industry share from 15% up to 20% of the region's value added (Roland Berger, 2014).

Open innovation and open source development:

Another opportunity is the promotion and support of open source developments from European players. A study from OpenForum Europe and Fraunhofer projected that an increment of 10% in open source collaboration from the EU could generate an additional 0.4% to 0.6% GDP as well as 600 new ICT startups (European Comission, 2021). Further information can be found in section 5.3.1.4.

European Digital Single Market:

The 'European strategy for data' contributes to the creation of a European single market for IoT. This strategy proposes policy and legal solutions concerning the free flow of data across national borders in the EU, and liability issues in complex environments such as the IoT one (Commision, 2021).

Potential to increase European influence in global standardisation fora and processes:

As one of the main takeaways from D1.1, standardisation strongly supports innovation and competitiveness, enables access to markets and interoperability, gives consumers confidence in innovations and further disseminates research results. As the future of IoT/Edge market points to global instead of regional standards, the next European research programme on IoT/Edge should take on this opportunity to be more active and encourage direct contributions to global SDOs & Industry Associations such as IEEE, IETF, ITU, ISO, IEC and TM Forum

Green Deal can contribute to accelerate digital transformation and IoT adoption:

One of the pillars of the European Green Deal is to stimulate innovation-based competitiveness. The plan is ambitious and will affect nearly every aspect of the EU's economy with proposals ranging from the automotive, aerospace, and maritime sectors to advanced materials or Internet of Things technologies which will benefit from acceleration services to support growth and scale (ClimateLaunchpad, 2020). One specific example of a niche to take on this opportunity is the role of IoT for earth observation, promising advances in data collection for the Sustainable Development Goals, including in the fields of climate change mitigation, biodiversity monitoring, poverty alleviation or smart agriculture (ITU, 2021).

4.7.5 Threats

Cyberattack vulnerabilities:

The threat landscape from the European Union Agency for Cybersecurity, ENISA, has pointed to an increase in the sophistication of cyber attacks. Malware stands in the first position, followed by an increase in Phishing, Identity Theft, and Ransomware (ENISA, 2020). The most affected sectors during 2020 were digital services, government administration and the technology industry (ENISA, 2020).

Strong competition from Asia and America:

As put by a DGAP report "*the primary front in the emerging tech power rivalry is between the US (United States of America) and China (People's Republic of China). The European Union (EU) has fallen behind and needs to catch-up*" (Sahin & Barker, 2021). This report also mentions artificial intelligence (AI), cloud computing, semiconductors, 5G and mobile equipment, and quantum technology as key technology areas of Europe's capacity to act.

Uncertain geopolitical landscape:

Taken from the market analysis annexed in D3.1, geopolitical uncertainty is an ongoing aspect to take into account as a possible threat to impact the European IoT/Edge R&D&I. Examples of this complex threats are the increasingly central role of technology in the transatlantic relationship with China (Pannier, 2021) or the reductions in FDI due to prolonged uncertainty (Santarsiere, 2019)

Dependency on non-EU suppliers (i.e. chips/hardware) & providers (cloud):

Supply-chain disruptions and rising US-China tensions linked to the European dependency on suppliers and other platform providers from these two countries raise the risk of a major impact on European companies. As Hobbs puts it in its article "*The EU cannot continue to rely on its regulatory power but must become a tech superpower in its own right. Referees do not win the game*" (Hobbs, 2020).

Freedom to operate & Dependency on non-EU IPR and patents:

China and other countries are massively patenting emerging technologies in the IoT, edge, cloud domain, that may restrict European innovation and freedom to operate of European SMEs and industry.

Strengths	Weaknesses
• Large funding and programme for research, innovation and deployment • Strong SMEs presence • Generally well educated human resources / people • Strong academic landscape • Existence of strong funding and programmes • Collaboration between European institutions, member states and research centres • Strong manufacturing and automotive industry • Cellular coverage and communications • Top leading 5G Cloud vendors • Widespread market adoption of consumer electronics • Privacy and security policies and culture • Strong expertise in data protection by design approach • Top journal publications • Active research community and mobility support • Strong expertise in public-private partnerships • Strong expertise in industrial data	• Market regulatory and linguistic fragmentation • Slow time to market (research to end-result process) • Missing digital skills to address the market needs • Lack of fertile ecosystems for startups and European industrial leadership • Bureaucratic and ineffective processes • Bureaucratic culture and lack of agility • Poor talent retention (brain drain) • Insufficient trust in cybersecurity and innovative technologies • Skepticism: resistance and fears with regards to digital transformation • Lack of standards, interoperability in IoT/Edge and adequate regulations in certain domains • Women in STEM still not always well regarded in some EU countries • Lack of IPR generation for building competitive advantages and raising VC investments • IPR patenting cost very expensive compared to other regions • Lagging in 5G deployments and adoption for IoT • Scarcity of European global industrial leaders
Opportunities	**Threats**
• IoT market expected to be a very large and fast-growing market • International adoption of data protection regulations & Regulatory evolution in data protection and cybersecurity which can constitute a competitive advantage • Digital transformation in all verticals & Era of digital manufacturing and industry 4.0 • Open innovation and open source development • European Digital Single Market • Potential to increase European influence in global standardisation fora and processes • Green Deal can contribute to accelerate digital transformation and IoT adoption	• Cyberattack vulnerabilities • Strong competition from Asia and America • Uncertain geopolitical landscape • Dependency on non-EU suppliers (i.e. chips/hardware) and non-EU service providers (i.e. Cloud) • Freedom to operate Dependency on non-EU IPR and patents

Table 2: SWOT Analysis Summary

The main takeaways in from the SWOT analysis in cross-cutting topics are:

- Europe has a certain number of strengths on which it can develop leadership in IoT, Edge and digital transformation. R&D are a strength in most cases, but Europe is less strong at transforming research into economic and industrial leadership. It is relevant to strengthen the impact and transfer of IoT-related research results to industry and market exploitation in Europe.
- Europe is depending on non-European supplier in several domains, as seen also in Figure 16. IoT/Edge blurring lines, like platforms, cloud services, hardware manufacturing, etc. This raises the question of its technological sovereignty. If the research programme focuses only on IoT services and application layer, it misses the opportunity to play a central role in the IoT industry.

- Development of open innovation through open source hardware and software are key opportunities for Europe according to a study on the impact of open source in the EU (European Comission, 2021).
- Europe is underrepresented in global IPR and patenting related to Cloud, edge, IoT and may face issues in terms of freedom to operate and risk to depend on non-EU IPR with associated royalties costs.

Europe has the opportunity to leverage on its Digital Single Market, the General Data Protection Regulation, and the Green Deal to take the lead in digital transformation by developing and bringing to the market innovative technologies and solutions. It would make sense to address these opportunities in the next calls for research on IoT and on the continuum Cloud, edge, IoT.

5 IOT-EDGE RESEARCH, INNOVATION AND DEPLOYMENT PRIORITIES

5.1 Consolidated Economical and Societal priorities linked to IoT in Europe

This chapter builds on the NGIOT scoping paper[78], the IoT and Edge report[79] and the IoT R&D&I priorities in the EU whitepaper[80] presenting an overview of the most important challenges in the IoT domain from an economic and policy perspective:

5.1.1.1 Support for SMEs and start-ups (E1)

SME enterprises in Europe are the core financial driver of growth[81], thus Europe needs to ensure their smooth transition towards innovative solutions, including IoT technologies. The adoption of IoT brings added value to companies and it has the potential to give SMEs a competitive advantage. Companies which will not be able to adopt IoT appropriately might suffer and 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 afor to develop their own solutions, nor use a strong and well-established brand (e.g. like Amazon, Google etc.) for other reasons like lack of trust, knowledge or skills. IoT4Industry signals 5 main barriers: lack of competences, regulation, unknown benefits, transparency, and mindset[82].

Additionally, it is crucial to support start-ups (e.g. providing access to business angels, investors, VC funds, accelerators, supporting partnerships with big players within that industry), as start-ups have the capacity to disrupt the market and to push innovation into new sectors in agile ways. However, it is not easy to find attractive IoT start-ups. Most of IoT start-ups fail to show a substantial recurring revenue stream, their revenue is often based on project-based consulting fees or through the support of one-time proof of concept (PoC) implementations rather than highly scalable software[83].

Supporting SMEs and start-ups can be rather difficult because of this, but it is still the best alternative for Europe to limit market monopolisation by the major and well-established players and at the same time strengthen European innovation in IoT domains. An SME Strategy for a sustainable and digital Europe[84] promotes concrete actions to support SMEs (as the heart of EU industry) toward a sustainable digital transition. This strategy is based on three pillars: capacity-building and support for the transition, reducing regulatory burden and improving market access, and improving access to financing.

5.1.1.2 Data and information as critical assets (E2)

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

---

78 NGIOT. https://www.ngiot.eu/report-iot-and-edge-computing-opportunities-for-europe/ (2021)

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

80 NGIOT. https://www.ngiot.eu/wp-content/uploads/sites/73/2020/09/D3.1.pdf (2020)

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

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

83 IoT Analytics. IoT Investments 2018 (2018)

84 https://ec.europa.eu/info/sites/info/files/communication-sme-strategy-march-2020_en.pdf

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.

5.1.1.3 Increase of digital skills and competencies (E3)

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.

The lack of qualified people is a challenge across all sectors in Europe. Initiatives that ensure capacity building in emerging technologies in the industry, SMEs and the public sector as well as specialised education at all levels are crucial for Europe's competitiveness and for ensuring that European key industry can continue to grow and stay competitive.

5.1.1.4 Build Trust (E4)

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.

5.1.1.5 Identification of the Key Regulatory and Legal Issues (E5)

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.

5.1.1.6 Interoperability and Replicability (E6)

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, the aim is to go towards common harmonised data models, starting with ensuring accurate interoperability at the semantic level. Following harmonised data models, harmonised functionality should be the focus. 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, such as proper and formal process modelling, engineering and execution technologies (e.g. TM Forum develops services and technology agnostic operational management APIs and testing capabilities, and the OMG standard Business Process Modeling and Notation (BPMN), is a formal business process modelling language that is executable). The effective integration of cross-domain data in business and organizational processes is another aspect, an initiative under this priority is the Smart Data Models initiative led by FIWARE, IUDX, OASC and TM Forum.

Alternatively, and also considering legacy or existing data models, ensuring proper semantic interoperability across ecosystems via appropriate techniques should also be considered, and especially as automated tools can be explored. An example here is the work in the One Data Model liaison group[85].

Also, under the umbrella of Gaia-X, work is conducted to push for interoperability Project GAIA-X' as the cradle of an open, digital ecosystem where data can be made available, securely collated and shared while enjoying the trust of its users. For edge in particular, interoperability is a way of avoiding fragmentation and overcoming the proliferation of different approaches at the infrastructure / orchestration level.

5.1.1.7 Innovation procurement (E7)

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.

5.1.1.8 Sovereignty (E8)

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. In terms of hardware, the recent global events have exposed a dependency from overseas providers now impacting directly the supply of microchips in many domains. The chips shortage in the automotive sector together with the digitisation of motor vehicles and the transition to zero-emission mobility (ACEA, 2021) is just one example of a clear need to create an European chip ecosystem, strengthen, in order to enhance reliability and avoid disruptions.

5.2 Consolidated R&D&I priorities linked to IoT in Europe

As result of the analyses of different roadmaps and the engagement with the community at different events, and taking into consideration the latest disruptive technologies, NGIoT identified the following high-level research challenges for the next work programmes. As

[85] https://onedm.org/

earlier discussed in Section 2, IoT, in its wider notion, is not a technology per se, but rather a combination of existing technologies, so it comes with no surprise that evolving IoT requires the evolution of the underlying technologies, including: 5G, Distributed Ledgers, Big Data, Artificial Intelligence, Cyber Security, and Cloud Computing. It is also important to highlight how 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. In this new version of the deliverable, for sake of clarity and in alignment with the approach used in the white paper "IoT and Edge Computing: opportunities for Europe" , we reorganize the priorities in relation to their main reference technology, while surfacing priorities that are specific to IoT research as System of Systems.

5.2.1 Internet of Things

5.2.1.1 Autonomous IoT solutions (R-IOT.1)

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

As part of this research area, NGIoT identified two major topics:

- **Large IoT & digital infrastructures (R-IOT.1.1).** Within Europe there is yet a lack of large deployments of IoT networks and digital infrastructures in general. This, beside slowing down the digitalisation process, also limits the ability to understand and test pratically implications of very large real life deployments of IoT infrastructures. This also relates to the unavailability of widely distributed public edge infrastructures that would allow to benefit OPEX model to IoT edge infrastructure investments. A potential research direction would be enablement of edge-federations and edge resource sharing solutions. Clearly this research topic is deeply linked with advancement in the are of data management and cloud computing, in relation to edge support (c.f. R-DATA and R-CLOUD).
- **Autonomous IoT infrastructures (R-IOT.1.2).** Due to the heterogeneous nature of the IoT infrastructure, which includes a variety of edge nodes with different resources, capabilities, mobility, ownership, etc. managing and operating IoT infrastructure at scale is more and more complex. Research is required to increase the automation in the whole cloud-edge-device management continuum to increase efficiency and reliability of IoT infrastructures. Machine learning and Artificial Intelligence may provide essential instruments to achieve such automation. It is important to evidence that IoT is introducing novel requirements to the cloud-edge continuum management, given that in more and more scenarios, IoT solutions may become dynamic ecosystems, thus required dynamic composition of edge resources from multiple owners. Such composition should occur preserving isolation of different users and privacy of data by the different stakeholders leveraging shared edges. Clearly this research topic is deeply linked with advancement in the are of data management, cloud computing and cybersecurity (c.f. R-DATA, R-SEC and R-CLOUD).

5.2.1.2 Human and sustainable development in the loop IoT (R-IOT.2)

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

As part of this research priority, NGIoT identified four major research topics:

- **Sustainable IoT by design (R-IOT.2.1).** A sustainable approach to IoT requires exploring solutions such as low power IoT devices and novel technologies for environmentally sustainable devices and sensors. Recent research also took into consideration the service side of resource efficiency, bringing into the picture energy-aware IoT service composition. "Sustainability" of course has a broader meaning and, in the case of IoT, covers as well other important aspects as well, such as resilient infrastructures, and inclusive access to technologies. So far research gave little attention to holistic approaches aiming at understanding how the different components of an IoT ecosystem contributes to make it sustainable, scoping from technologies to policies. Research should focu on study how the different layers of an IoT ecosystem can interplay to deliver sustainable IoT solutions, it should explore how systems can self-adapt to comply with sustainability KPIs. Innovative ways to incentivize Sustainable IoT policies are also to be explored.
- **Augmented IoT (R-IOT.2.2).** While augmented reality technologies are maturing, their adoption in conjuction with IoT is still limited. The relevance of Augmented Reality for IoT is linked to the ability to allow humans to interact with data generated by IoT devices and devices themselves in a similar way to the one humans would interact with the physical world by "augmenting" it. The combination of Augmented Reality with Internet of Things and Artificial Intelligence to support human control and interact with "things" is still at its infancy and its key to for the development of advanced Digital Twin solutions. Research should explore not only solutions to enable Augemented IoT, but also socio-ethical aspects linked with the transition toward such novel type of interactions with the physical world.
- **Tactile Internet (R-IOT.2.3).** Human sense are able to interact with the physical environment at incredible speeds. While a muscular reaction is in the range of 1sec, human visual reaction is in the range of 10 msec. Thus while interacting with "things" humans expact reaction times compatible with their senses capacities. Tactile Internet research explore solutions to provide such "low latency" and "human-sensible" interactions (e.g. leveraging haptic feedback) with the ultimate goal of empowering humans to control remote "things" via Internet like real physical objects. Tactile Internet thus enables precise human-to-machine and machine-to-machine interaction key to several scenarios such as in manufacturing or in healthcare. Requirements of the Tactile Internet place extraordinary demands on networks' latency and reliability, security, IoT architecture, sensors and actuators. Research in the area is still in its infancy and 5G/6G

research progress are not yet at point of providing end-to-end latency below 1 msec in remote control loops, still relevant progress in research for haptic interactions and augmented interactions have been done. Leveraging on Photonics technology to reduce latency in both the communication and sensing/interaction layer may be key to achieve the Tactile Internet vision.

- **IoT for sustainability (R-IOT.2.4).** IoT-based solutions can improve the sustainability of different economic sectors such as manufacturing, agriculture, and smart cities. This line has been deeply explored and the applicability of IoT to improve efficiency of processes and reducing resource usage, is now considered a fact. Research exploring impacts on other scenarios, such as social inclusion, is starting to take up as well with major focus on impaired and ageing people.

5.2.2 5G & 6G networks

5.2.2.1 Reliable, low-cost, sustainable and scalable IoT networks (R-NET.1)

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

As part of this research priority, NGIoT identified two major topics:

- **Low-cost, high-volume connectivity (R-NET.1.1).** Research should explore radio transmission solutions that, while increasing bandwidth available for IoT data transport, would reduce the cost of deployment of the radio networks. In particular, interesting areas of investigations are: new frequency bands (e.g. unlicensed band > 200 GHz), new medium for signal propagation (e.g. single mode optical waveguide using laminated polymer platform). Light Fidelity communication technology and its convergence with 5G should be further explored as well.

- **Low-power connectivity schemes (R-NET.1.2).** Hardware and software solutions should drastically reduce the energy consumed by IoT devices to collect and transmit information. Software solutions and communication protocols may optimize activation of communication and consumption during communication, while energy harvester and other bio-inspired solutions may increase the capacity of batteries and energy independence of devices.

5.2.3 Data Management, Artificial Intelligence & Machine Learning

5.2.3.1 Next Generation IoT data processing architectures (R-DATA.1)

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 rethought, 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).

Considering the potential massive scale of IoT with 10Bs or even 100Bs of data sources and sinks, combined with an increasing need for (near) real-time insights where they are needed in the topology, the traditional separation of network, cloudification and data processing architectures can become a barrier for growth. In light of IoT becoming hyperscale, architecture approaches that flattens or even remove these separations should be exploited towards a "network compute fabric"[86]. This would also allow for having IoT data processing (data aggregation, sensor fusion, inferencing) effectively embedded in the network topology and even accelerated by dedicated hardware like Graphics Processing Units (GPUs), and Tensor Processing Units (TPUs) embedded in the network itself for use by applications. Proper network-native data pipelining technologies combined with "Function as a Service (FaaS)" approaches would further enable this fusion of network, cloudification and data processing. In short, IoT data processing architectures need to be scalable by design.

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.

The major complexity in the area relates to i) the complexity of splitting and synchronizing the data processing tasks in the computing continuum while ensuring their overall reliability, availability and performance; ii) making available in a seamless way the different processing tasks to a variety of computing platforms, spanning from the cloud to embedded devices.

In this context, two major research topics have been idenfied :

- **Highly scalable and low latency ledgers for IoT (R-DATA.1.1)**. In more and more IoT scenario, distributed ledgers are key enablers for secured and trusted data exchange and distributed processing. However, their application in real time scearios is still not possible given that current distributed ledger solutions introduce additional latency in

[86] https://www.ericsson.com/en/edge-computing/network-compute-fabric

the data management and have high computing costs. Proper solutions need to be explored to allow adoption of distributed ledgers at the scale and latency required by real time IoT scenarios.

- **Unified processing paradigm (R-DATA.1.2).** Most of the data processing solutions in place today are cloud-native and supports to a certain extent distributed processing (from edge to cloud). Still, these evolutionary solutions are not mature and more research investments are required to complete the extension of existing technologies and approaches to incorporate edge processing. The major limitation is that these solutions are not designed to deploy and orchestrate data processing task in a seamless way on cloud and embedded devices. In this sense, research should explore novel mechanisms for data processing, looking beyond current consolidated solutions. Promising trends that could support such evolution include: function-as-a-service, that recently introduced support for edge-cloud orchestration; distributed in memory-databases that offers unmatched performances compared to traditional distribteud databases; solutions, such as web assembly, that enable, virtually to port the same data processing task on any hardware architecture. Open source solutions such as FAASM[87] are paving they way in this direction.

5.2.3.2 Decentralised machine learning (R-DATA.2)

With the advent of edge computing more and more we witness the need for distributed machine learning approaches, where inference and training occurs distributely. In this context, Federated Machine Learning research is playing a major role, enabling the (centralised) creation of models from partial training, thus without requiring data set sharing, and hence ensuring data privacy and security. More advanced techniques going under the name of Swarm Learning builds not only on decentralised data, but also on decentralised models, being the only element shared across actors the hypertuning parameters. In both cases, the efficiency and speed of the communication between the nodes is affected by network latency issues, and requires techniques to « minify » the information shared. The roles of these new decentralised techniques and optmised models for decentralised ML is complemented by raising approaches for Machine Learning Operations that foster the adoption of techniques similar to the ones adopted in DevOps context to automate the lifecycle of machine learning solutions.
In the short-medium term, research should focus on novel approaches to reduce computational and data transport requirements of computing and executing AI algorithms. In the longer term, research should look into disruptive approaches that will handle barriers of today architectures. This research is instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

In this context, three major research topics have been idenfied:

- **MLOps and decentralised AI/ML pipelines (R-DATA.2.1).** With the advent of edge computing, AI processing is moving from the cloud toward the edge, allowing for fast local decisions. To make this possible it is key to explore decentralised mechanisms to orchestrate AI pipelines, i.e. the process of collecting and adapting data for model computation, the model computation and their deployment. Such pipelines will need to i) embrace MLOps able to trigger model re-computation, not only based on analyed data, but also on the application contextual data, and to ii) integrate ways to preserve data privacy in complex and distributed IoT ecosystems (e.g. by leveraging federated

[87] https://github.com/faasm/faasm

machine learning architectures). Decentralised AI/ML pipelines will have a key role to increase data privacy.

- **Lightweight AI and ML (R-DATA.2.2)**. While the "divide et impera" approach is essential to support distributed/decentralised computation, it may not be enough to support the training of algorithms and their deployment in low power devices at the edge. Approaches that have a small computational and data transport footprint both during the training phase and the inference phase are essential to enable intelligence in the case of low power devices. In this sense research approaches, like the one of TinyML provide interesting solutions that in combination with decentralised AI architectures may scale in the cloud-edge continuum. These approaches should be complemented by the techniques to compress models and optimizing them[88], so as to reduce the network traffic volume and novel over-the-air transmission techniques[89] for federated learning to effectively reduce the communication and energy expenditure.
- **From federated machine learning and swarm learning (R-DATA.2.3).** Thanks to the increasing maturity of federated learning solutions (see for example open source solutions such as TensorFlow Federated[90] and Flower[91]), the adoption of decentralised solutions for machine learning is increasing. These solutions adopt techniques based on decentralised training that is then leveraged to centrally compute a model that. Essentially, the only parts decentralised of the machine learning lifecycle are the training part and the inference, while model computation and serving remain centralised. While this a greate step ahead in term of data privacy, data security, and reducing data transfers, it still require an established trust between the parties involved, given that in the end the control of the whole machine learning lifecycle is centralised. To overcome this limitations, an new promising research directions is swarm learning (Hüttenrauch, 2019; Warnat-Herresthal, 2021), where learning occurs in a trustless and cooperative way based on pre-agreed rules (for example via ledgers and smart contracts). In the context of swarm learning, models are computed locally based on local data, without a central controller. Parameters are extracted from the models and shared across all the swarm nodes in a peer to peer fashion, and used to re-optmize local models. This research area is still at its infancy but seems very promising to enable decentralised intelligent IoT solutions.

5.2.3.3 Trusted and effective decision for IoT solutions (R-DATA.3)

Machine Learning and Artificial Intelligence are more and more being part of solutions deployed in the market to increase automation in several IoT application area, such as autonomous vehicle, automated cropping, and so on. 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). Morevoer, while the number of AI solutions is increasing it remain important to evaluate the quality and effectiveness of computed models. Accessing

---

[88] S Wiedemann et al. (2020), DeepCABAC: A universal compression algorithm for DNNs. IEEE Journal of Selected Topics in Signal Processing

[89] Liu, W., et al. (2020). Over-the-air computation systems: Optimization, analysis and scaling laws. *IEEE Transactions on Wireless Communications*, *19*(8).

[90] https://www.tensorflow.org/federated

[91] https://flower.dev

quality models is particularly important to develop effective solutions and access to the mass of data required to compute such models is a key market barrier, especially for small players.

This research priority is multi disciplinary in its essence and encompasses ethics, socio-economic and psychology.

As part of this research priority, NGIoT identified four major topics:

- **AI for Humans: understandable and ethical decisions (R-DATA.3.1).** While humans could easily understand first AI systems, recently the adoption of deep learning models such as Deep Neural Networks (DNNs) is raising and increasing the opacity of AI systems. At the same time, users interfacing with AI systems are more and more demanding for transparency. To answer this need, research focused on eXplainable AI (XAI). XAI leverages social sciences (e.g. psychology) to define a suite of machine learning solutions that produce easy to explain models so as to enable their understanding by humans. Making models human understandable is the first step toward trust of AI and ensuring its compliancy with ethics, i.e. toward responsible AI. Research in XAI and similar approaches required advancemnts in order to achieve same performance as "black-box" machine learning systems and increase the adoption in IoT solutions.
- **Validated AI algorithms for IoT use cases (R-DATA.3.2).** While there are a number of models discussed in research papers in relation to different use cases (e.g. pest detection in agriculture, object and vehicles identification in smart mobility) rarely these template models are tested at scale and made available freely and openly. Stakeholders capable of generating (or having access to) large enough data sets to compute accurate and efficient AI models are generally keeping them closed source, thus limiting the impact and benefit for society and the possibility to verify and validate the models (also within respect ethics issues). To the aim of releasing to the wide public free and open high quality AI models, a singergy with data market places is key (cf. Rx.2).

5.2.3.4 IoT, processes, and data Interoperability (R-DATA.4)

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

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

- **IoT data dictionaries deployed at scale (R-DATA.4.1).** One of the key solutions to ensure intereoperabilty of IoT solutions, is the adoption of common and standardised dictionaries. While a number of efforts taclked the definiont of such dictionaries in relevant scenarios, the coverage of scenarios is still limited, and worst the adoption of such dictionaries is often limited. Activities should focus on increasing available dictionaries and their adoption.

- **Semi-automated data interoperability (R-DATA.4.2).** Several IoT solutions deployed on the market are specific to a given domain. This trend contributed to creation of so called data silos. This makes quite complext the seamless integration and intelligent analysis of the various heterogeneous data sources. In the past solutions based on semantic technologies have been proposed, and while they worked well conceptually, the had several issues of scalability and performance. With current evolution of deep learning techniques should be explored to provide automate as much as possible annotations and transformations.

  Semi-automated process interoperability (R-DATA.4.3). If attempts to automate data interoperability proved so far unefficient and not scalable, the state of the play for processes it is even more complex. Still, such interoperability is key to increase the dynamic integration of different IoT platforms enabling ecosystem of IoT data consumption and production.

5.2.3.5 Data sharing and monetisation enabling models and technologies (R-DATA.5)

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

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

- **IoT data market architectures (R-DATA.5.1).** Differently from centralised data market architectures that can be applied in several scenarios, in the case of IoT scalability may be achievable only with decentralised and distributed approaches. Distributed ledgers, while offering a decentralised approach and providing solutions increasing data control by owners, have yet to mature and achieve performances required by realtime IoT scenarios. Efforts and experiments have beed done in this direction, for example, by IOTA and Streamr to develop IoT data market places based on IoT native distributed ledgers.
- **Novel business models to incentivise data sharing (R-DATA.5.2).** While data sharing could provide huge benefits to the whole society, successful examples of data market are very limited. Sensor data sharing markets such as Streamr, Dawex, and QueXopa are still low populated. Companies are reluctant to sell their data, since they cannot easily evaluate the monetary value of the data to the purchaser and consequently are afraid of setting a price. Another, perhaps more obvious reason is that many companies are afraid of their data being used against them. In the data economy context, platform cooperatives have been proposed and implemented with the purpose of tilting the asymmetric distribution of power to affect platform rules, and the distribution of value, towards more symmetric and equitable arrangements. Often the value of the data cannot

be determined when a data provider and data consumer agree on the use of the data, but only when the data are actually used by the data consumer. These demands for new governance models - or new kinds of agreements - that define how the value of the data is evaluated at the time of its use, how the created value is shared or divided, and what are the rules for the parties for extracting or monetizing the value. This may lead to new compensation models different from the typical one-the-spot monetary compensation.

- **Large data marketplaces for IoT scenarios (R-DATA.5.3)**. While as mentioned above IoT data marketplaces have been experimented in different use cases, so far they haven't reached the critical mass that would allow them to generate value for the stakeholders involved. Public investements, such as the ones envisioned in the EU Data Strategy, may be able to mobilize the scale needed to create such market and make them sustainable.

5.2.4 Cloud architectures

5.2.4.1 Self-* for edge computing (R-CLOUD.1)

One of the key characteristics of determining the success of cloud services are their self-* (scaling, healing, …) capacities. These automation capacities are yet to be taken at the whole cloud-edge-device management continuum. Machine learning and artificial intelligence may provide essential instruments to achieve such automation, that is not yet embodied in any of the reference cloud-native orchestration solutions available in the market today. Additionally, such orchestration capacities should as well tackle more and more important aspects in infrastructure management such as energy impact. Initiatives (such as KubeEdge, microk8s, and k3s) around Kubernetes ecosystem are aiming at empowering its usage at the edge, still not all devices available at the edge may be able to host solutions like k8s, and research and development toward more holistic approaches are required.

5.2.4.2 From centralised orchestration to collaborative orchestration (R-CLOUD.2)

Due to the heterogeneous nature of IoT infrastructures, which include a variety of edge nodes with different resources, capabilities, mobility, ownership, etc. managing and operating IoT infrastructure at scale is more and more complex. More, IoT is introducing novel requirements to the cloud-edge continuum management, where in more and more scenarios, IoT solutions may become dynamic ecosystems, thus requiring dynamic orchestration and composition of edge resources from multiple owners, and moving from current federated approaches (such as the one proposed by GAIA-X acting as a central authority) toward more peer-to-peer approaches (not requiring a central authority). Such orchestration and composition should occur preserving isolation of different users and privacy of data by the different stakeholders leveraging shared edges. In this respect, approaches like swarm computing (ATOS, 2018), leveraging on swarm learning approaches, clearly provide a promising direction.

5.2.4.3 Energy aware cloud-to-edge infrastructures (R-CLOUD.3)

While energy efficiency and awareness (i.e. taking decision based on the energy source or demand) have been largerly explored in data centers, leading to a clear picture of how an energy and computation relates in a closed environment, a clear understanding in the case of the open internet where cloud-to-edge solutions operate is yet to be developed. A fundamental requirement to understand phenomena is the ability to measure it, looking at cloud-to-edge infrastructure combining multiple operators and networks, we are not yet able to measure end-to-end the energy consumed. This is due to the fact that: i) energy efficiency in the data centers is mainly meant for the operators, generally no information is shared to the actors that acquire cloud resources to provision services; ii) in the cloud-to-edge scenarios, the network play a major role, and information on “real time” energy consumption of a given streaming of data is not only not shared by the operator, but beacuase it is even very complex to compute or model, and as results estimation of the energy related to data transport vary a lot. While research is attempting to provide answers and models to enable the creation of energy aware cloud-to-edge infrastructures, a fundamental pre-requisite to ensure the efficiency of such solutions is the availability of data, and hence standards to expose energy related information from the cloud to the edge, and policies to enforce providers to expose such information to the developers, as today occurs for other infrastructure metrics, such as CPU and memory load. Advacement in this direction are key to ensure that with the increased adoption of edge computing for IoT solutions the energy efficiency is compromised, rather than been improved as envisioned by policies related to the area.

5.2.5 Advanced electronics

5.2.5.1 Sustainable and biocompatible devices (R-ELET.1)

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

As part of this priority, NGIoT identified two major research topics:

- **Energy efficient devices (R-ELET.1.1)**. Early studies indicate that the combination of micro-energy harvesting and micro-storage technologies may be the future for long lasting IoT devices. Improving their combined performance while downscaling their size can only be achieved through breakthroughs in materials performance and system architectures that allow for high density features and embedded energy options in integrated circuits (ICs) .
- **Sustainable devices (R-ELET.1.2).** While energy efficiency is key to reduce the impact of IoT on the carbon footprint, it is not the only aspect that influences IoT device “sustainability”: the shift toward the edge is going to increase the number of devices, thus potentially increasing the linked “digital waste”. Devices need to be designed in such a way that their lifecycle environmental impact is close to zero. Recent research showed the great potential for the improvement of the devices' design holding by nano- and biomaterials invented in the last decade. Research should advance toward minimally invasive electronic devices embedded directly into biological objects. Such hybrid systems may enable high-quality, low-cost sensors as an alternative to more expensive fully electronic devices. IoT applications will benefit from using hybrid bio-electronic sensors which rely on natural capabilities of bio objects (e.g., bacteria, plants, animals) and react to changing environments.

5.2.5.2 High performance computing devices for the edge (R-ELET.2)

Nowadays cloud offer includes different specialised capacities, including GPUs and other AI and ML specific hardware design allowing to speed up training and inference in the cloud. Clearly, there while there is space for research and improvements in the AI-enabled computation in the cloud, the major research challenge of today reside elsewhere.

With the increasing need for low latency processing capacities, more and more we witness the move toward the edge of computing. This, on the one side, posses several challenges in the way distributed processing is orchestrated (as previously discussed). On the other side, edge computing to provide low latency not only require to be localise close to the data or the user, thus reducing the network latency, it requires as well powerful computational capacities to be available in devices that have constraints on their size and their energy consumption.

- **Native AI-capable edge devices (R-ELET.2.1).** To improve performance of IoT-related data processing and decision making, developing devices with novel processing capacities is key. In particular, advancements in AI specialised processors are required. Good progress has been made toward processing units capable of performing machine learning and deep learning tasks at the edge. Current research shows that AI specialised processors can achieve 10 times the performance of GPUs and FPGAs. Still this capacity may not be enough with the increasing volume of data that will be generated and new research developments such as neuromorphic computing should be investigated. While achieving this goal, research should also ensure that energy usage is keep under control (c.f. R-ELET.1.1).

5.2.6 Cybersecurity

5.2.6.1 Futureproof security and trust (R-SEC.1)

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

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

- **AI-powered cybersecurity (R-SEC.1.1).** Research in cyber security explored supervised and unsupervised machine learning methods such as Random Forest (RF), SVM (Support vector machine), decision trees (DT), k-nearest neighbour (KNN), k-means, Principal component analysis (PCA) and association rule (AR) algorithms have been widely adopted in cyber security (Kaloudi, 2020). Their ability anyhow to detect an attack is strictly related to the attack patterns identified in the past. More recently, initial attempts to leverage deep learning and reinforce deep learning provided interesting results in the identification of IP Spoofing and DDOS. Such methods seem promising since they have been able to recognize attacks that were not showing similarities with previous attack patterns. Research in this direction is key to increase resiliency of IoT platforms in the cloud-edge continuum.
- **Data traceability and trust in the cloud-edge era (R-SEC.1.2)**. Data traceability is a key step to increase trust over data. In particular, taking into account security concerns linked with IoT devices, the tracing provenance of data and the usage of solutions that

guarantee that data have not been tampered is essential to increase trust toward IoT systems. Distributed ledgers are becoming the reference solution for data traceability in different scenarios, including, for example food provenance and circular economy (Zhu, 2019). While distributed ledgers have been applied to IoT to increase trust, current protocols are still limited in terms of scalability when it comes to large scale sensor networks. Higher scalability of consensus protocols are needed in the cloud-edge era. Different solutions are promising, including the ones explored by EU initiatives such as IOTA, and mixed approaches that combine ledgers with DHT overlays (e.g., Chord, Pastry, and Tapestry).

5.2.6.2 Privacy-by-design (R-SEC.2)

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

As part of this research priority, NGIoT identified two major topics:

- **Privacy-by-design for IoT devices (R-SEC.2.1**). Devices are considered one of the more exploitable entry doors for cyber attacks. Thus it is essential to advance research related to their security, including solutions for on-chip encryption, hardware-software integrated security functions, tamper proof technologies. While privacy by design in the are of data is largely explored (D'Acquisto, 2015), additional research on device privacy is required to increase trust toward IoT (Seliem, 2018).
- **Security & Privacy-by-design for IoT services (R-SEC.2.2).** Recently there have been more and more breaches of sensitive data, and attacks on critical infrastructures. Increase security of IoT infrastructures is central to the safety and security of several applications and their users. On the security side, it is fundamental that research strengths methods for development of secure architectures including new methods and tools for formal verification of specifications, designs and implementations to detect possible security threats. Artificial Intelligence (cf. R-SEC.1.1) may play a key role into supporting such methologies and in the development of cyber threat solutions (model level proofs, source code analysis, binary analysis, hardware analysis, etc). As regards privacy, many research aspects are yet to be explored, including: ways to automate GDPR compliance tests, solutions to provide privacy preserving data processing and machine learning (for which distributed ledgers may provide interesting solutions), mechanism to generate dynamically data access control policy based on different context parameters while preserving data privacy.

5.3 Consolidated strategic priorities linked to IoT in Europe

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

5.3.1.1 Standardisation in IoT (S1)

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

The creation of value and the IoT trust framework: In order to facilitate the growth and development of the IoT market and value chain, two fundamental elements are the adoption of a "trust by design" approach, together with sustainability in mind. We have already seen in the section devoted to societal challenges why the security and the protection of privacy needs to be build in as key features in IoT deployments. As regulation is fragmented along national lines (e.g. GDPR is implemented with slight differences across Europe), different stakeholders have taken an initiative for the creation of an IoT trust framework to raise the level of security of IoT devices and related services. The framework developed covers different areas focusing on the following principles: authentication, encryption, security, updates, privacy, disclosures, control, communications. The framework identifies core requirements that manufactures, service providers, distributor/purchasers and policy makers need to understand and embrace to develop a trust framework for the IoT[92]. IoT platforms and the development of the IoT value-chain should address, by design, trustworthiness, data privacy and data security; and integrate sustainability models.

5.3.1.2 IoT and the Digital Single Market (S2)

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

---

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

in complex environments in order to enhance legal certainty and trust in complex environments such as the IoT one. According to the European Commission the value of the data economy will increase to EUR 643 billion by 2020 representing 3,17% of the overall EU GDP.

5.3.1.3 5G and IoT (S3)

The transition of many companies and organizations towards adoption of IoT will also be grounded in the adoption of other key technologies such as the fifth generation of wireless technologies (5G). 5G offers to corporates important benefits in terms of data speed, latency, reliability, efficiency, capacity and security. 5G is therefore expected to support a wide array of new solutions. As highlighted by KPMG: "Some of the benefits of IoT could be realized within an existing telecommunications infrastructure, but previous wireless technology generations do not have the capability to integrate with autonomous robots or advanced technologies. In contrast, when IoT is combined with 5G networks in a transformation strategy, the goals of i4.0 come within reach"[93]. The deployment of 5G will therefore constitute a building block of the Digital Single Market and the European Union has already taken several initiatives already from 2013 by establishing a Public Private Partnership on 5G (5G PPP) and by funding several research and innovation projects. 5G standards are also one of the five priority areas under the European industry initiative. The 5G Action Plan for Europe was adopted in 2016 with the goal of starting the deployment of 5G services in all the EU Member States by the end of 2020. Given the market relevance of 5G deployments the European Commission launched also the European 5G Observatory in 2018 to monitor major market developments in a global context. For the development of proper market solutions, the role of Member States has to be taken into account as well, for this purpose a report on national strategies and their consideration under a European perspective has been published. 5G deployments are to be considered in a market perspective also from a security and geopolitical, for this reason a coordinated risk assessment was undertaken.

5.3.1.4 Open Innovation role (S4)

A fruitful interaction between IoT growth and the role of open innovation brings new opportunities and innovations to companies and to society. Open source enables open innovation and open collaboration and creates a huge opportunity to strengthen European leadership in IoT and Edge Computing. A recent study from Open Forum Europe and Fraunhofer projected that an increment of 10% in open source collaboration from the EU could generate an additional 0.4% to 0.6% GDP as well as 600 new ICT startups (European Comission, 2021).

The potential for European leadership is highly connected to the capability of developing and promoting open source, industry-grade software platforms as those platforms allow research organisations, SMEs, and large organisations, to collaborate on core technologies and leverage those technologies to support their researchers, or to enter the market with innovative products built on top of the platforms. Figure 27 below shows how this approach has been formalized and implemented by the Eclipse Foundation, especially in its IoT, Edge Native and Sparkplug working groups[94]. Together, they regroup 50 projects and over 55 member organizations.

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

[94] Eclipse Foundation. IoT Commercial Adoption Survey 2019 Results (2019)

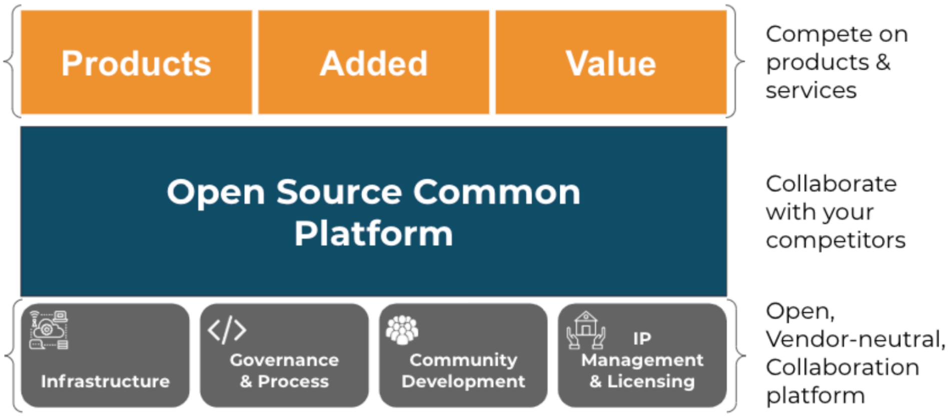

Figure 27. Eclipse Foundation approach to open source platform

Open source is specifically adapted to the challenges of IoT and Edge Computing as it enables scalability and interoperability, fosters collaboration and adoption, and creates trust. Scalability and interoperability are two characteristics of open source platforms that result from the core characteristics of the openness, royalty free licenses, and of the capability of studying code that ensures better interoperability. Openness is a pillar for the development of an interoperable, sound and trustworthy ecosystem. Open platforms are a way to create open end-to-end frameworks for IoT which allow a trustworthy and reliable integration of AI. Open source is also an accelerator of adoption as developers can use new open source technologies and build prototypes without restriction. Finally, open source is an enabler of trust as it is possible to inspect the code in order to check its characteristics regarding security or privacy constraints.

It is worth mentioning that the 2019 Eclipse IoT Commercial Adoption Survey[57] found that the top three reasons mentioned by the participants to adopt open source technologies were control, cost and flexibility — in that order. Given the rigid constraints that most IoT and Edge Computing solutions have to operate under, it is not surprising adopters value the control open source technologies grant them.

Open Source platforms and open standards are global, and Europe, especially with the support of the strong European research ecosystem, can lead the charge in developing and promoting such Open Source IoT and Edge Computing platforms and standards, thus developing the skills and excellence and ensuring European leadership in the domain. Figure 28. The Eclipse EdgeOps Matrix shows key open source projects from the EdgeOps ecosystem where projects marked with the European Flag are mainly developed in Europe.

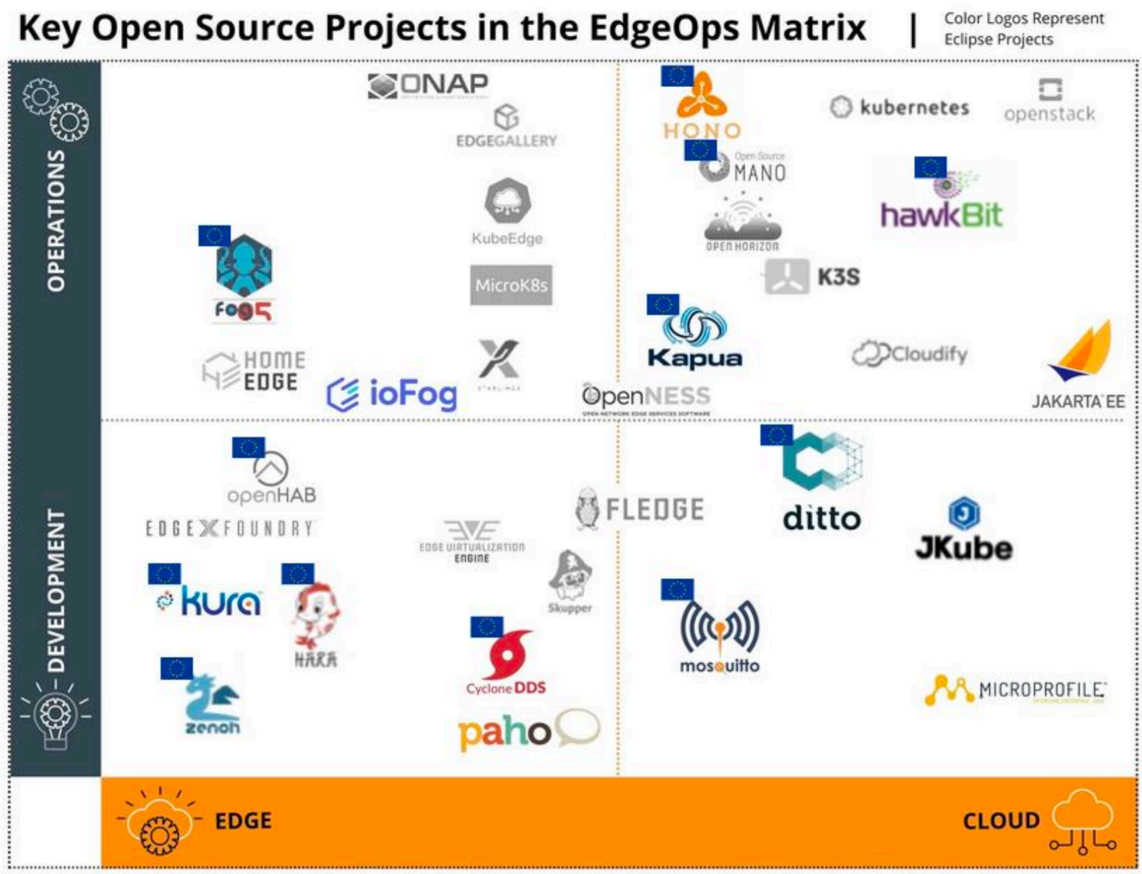

Figure 28. The Eclipse EdgeOps Matrix

This availability of open source technologies will allow various actors, including SMEs, to create products and solutions and enter the market with a strong competitive advantage if the underlying open source platform is widely adopted. Because of the importance of SMEs for the EU, academic research recommends that Open Innovation policies must move outside of the walls of large companies, fostering an open innovation environment that is equally beneficial for all[95]. However, policies should take into account the multiple challenges that SMEs face while implementing open innovation, which lead to uncertainty and even renunciation of open project participation[96].

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

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

5.3.2 Domain specific opportunities

5.3.2.1 Agrifood and Smart Farming

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

IoT and Edge Computing: Agrifood & Smart Farming[97]	
Current state, trends & opportunities	Challenges & barriers
Deploying IoT in the agri-food sector has proven to be **difficult despite market demand**, and the large number of **use cases** that would benefit from IoT. A successful digital transformation of the agrifood sector should include an **inclusive** approach to realise new scenarios from **farm to fork**. Acquired data can be transformed into knowledge that will facilitate control of farming activities (e.g. **health control, feeding, growth**) as well as enable an autonomous control of processes and activities along the **agri-food chain**.	• Widespread Connectivity • Trust • Security and privacy • Mindset and culture • Battery lifetime • High upfront costs • Accuracy of sensors • Fragmentation • Investments have long payback periods, low profit margins
Priorities and actions	Key organisations
Support for **digital innovation** through experimentation can guide the way towards a sustainable **integration** of Edge IoT in the supply chain from farm to fork There is a need for initiatives that create **trust and change culture** (demand side) The transformation of the agriculture sector calls for an inclusive, **partnership approach** and for interactions with and learning from experiences of other sectors in particular smart cities and communities (including **rural development**), logistics, the food industry, meteorological services and retail.	• CEMA • ECPA • CELCAA • COCERAL • COPA-COGECA • EFFAB • Euroseeds • FEFAC • EIP-Agri • AEF Relevant H2020 projects • Smart Agrihubs • IoF2020 • AGRICORE • DEMETER

[97] https://www.ngiot.eu/event/ngiot-thematic-workshop-rural-smart-communities-and-agrifood/?instance_id=119

5.3.2.2 Smart cities and communities

One of the domains, where IoT has an enormous potential is smart cities and communities. Monitoring and managing traffic and transportation systems, power plants, water supply networks, waste management, buildings, community services and others provide a solid basis for analysis and predictions, thus enabling cost optimization and effective allocation of resources.

IoT and Edge Computing: Smart cities & communities[98]	
Current state, trends & opportunities	Challenges & barriers
Edge as post cloud and multitenant technology, combining various data streams into personalized solutions for citizens Edge as a way to create inclusive and sustainable cities, as e.g. moving towards predictive/real time traffic optimization by enhanced connectivity of users, assets, vehicles and infrastructures. European ambition to deploy "10,000 climate-neutral and secure edge nodes" across the EU, open and distributed in a way that will guarantee access to data services with low latency wherever businesses are located.[99] European Mission on Climate-Neutral and Smart Cities, with the aim of 100 climate-neutral cities by 2030, and all 95,000 EU municipalities by 2050.[100]	• **Trust** (by end-users) • Security and privacy • Lack of interoperability • Vendor **lock-in** • Scalability • Inclusiveness

Priorities and actions	Key organisations
Embedding edge in cloud strategies Micro edge Swarm computing Shift to edge computing is a pathway to the green digital transformation of cities and communities Partnerships across the demand and supply side Open source adoption	• OASC • EUROCITIES • ENoLL • Artemis Industry Association • EPOMM • ELTIS • UTA • IoT Forum Relevant Initiatives

[98] https://www.ngiot.eu/event/ngiot-thematic-workshop-smart-cities-communities/?instance_id=120

[99] European industrial technology roadmap for the next generation cloud-edge offering,

[100] European Mission on Climate-Neutral and Smart Cities: https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/eu-missions-horizon-europe/climate-neutral-and-smart-cities_en

- Living-in.EU
- EIP-SCC
- JPI Urban Europe
- CIVITAS

Relevant H2020 Projects

- DUET – Digital Urban European Twins
- AURORAL
- dRural
- EIP-SCC lighthouse projects

5.3.2.3 Smart Health

The introduction of IoT in healthcare supports hand hygiene monitoring systems, remote health monitoring through wearable devices and smart medical apparatus manufacturing. The combination of smart sensors and cloud computing is used to optimise the flow of patients, staff, equipment and medical supplies hospital wide. This gives many opportunities for extension of revenue streams in the healthcare industry. Due to optimization based on dynamic data, it can reduce inefficiencies and enable better allocation of financial resources. Biometric wearables to track health and lifestyle provide important information concerning the tailored medical treatment as well as solid data for health insurance companies.

IoT and Edge Computing: Smart Health[101]

Current state, trends & opportunities	Challenges & barriers
Integration of IoT into the healthcare domain is **accelerating quickly**. Most patient interactions involve the use of medical equipment and devices. IoT brings visibility for healthcare professionals what is happening in such systems. EU has been updating its regulations of medical devices. Research domain to be addressed related to data **protection by design and by default**.	• Legal and regulatory compliance with the **GDPR** • Lack of interoperability • Connectivity • Trust • Security and privacy • **High costs** for research and development

Priorities and actions	Key organisations
A major priority for the eHealth domain is to **ensure data privacy and protection by design** and regulatory compliance (GDPR, NIS, ePrivacy). User **acceptance**, including by users with disabilities is another key requirement, which will require developing new pilots and adequate methodologies for **end-user engagement** in the research process. **Standardization and interoperability** are priority objectives to be addressed.	• MedTech Europe • EIP on AHA • ECHAlliancere • HL7 • AIOTI • IoT Forum • ECCP Relevant H2020 projects • GATEKEEPER • ODINS

[101] https://www.ngiot.eu/event/ngiot-thematic-workshop-health-and-care/?instance_id=148

5.3.2.4 Energy Management:

IoT technology can be employed to create smart grids that price and route power, based on the demand and prevent blackouts, amogst other applications related to all the energy sources. This leads to optimization of resources and better service.

IoT and Edge Computing: Energy[102]	
Current state, trends & opportunities	Challenges & barriers
Energy is a **critical infrastructure**. It is also a key sector to progress towards the **green transition**, and IoT and Edge are an important enabler of it. Currently, attempts are made to enable SCADA systems and connect them to the Cloud. With this approach, most of the logic still sits within large controllers, now supported by some further **intelligence in the Cloud**.	• **Scalability** (harmonised penetration across Member State) • Interoperability • Security & confidentiality • Reliability
Priorities and actions	Key organisations
Sustainability: Intelligently integrating distinct and distributed energy sources, and components using AI, IoT, Edge, Fog, Cloud computing, ensures flexibility to balance very large shares of renewables - and obtain substantial reductions in **CO2 emissions.** The role of Cloud - Edge architectures and 5G is crucial to offload computationally intensive operations to the Edge instead of the Cloud, allowing services like **transactive energy** approaches, which are the future of renewable **integration to the grid**. Cloud-Edge architectures with 5G communications empowers blockchain-powered energy networks. Digital twins could be used for mitigation issues: lower communication latency, faster development lifecycle (faster evolution of services), increased resilience, local data keepers. **New partnerships** are needed, **adoption of open source** and strengthening the ecosystem, including collaboration with SMEs	• EERA • ERA-Net SES • EURAC • COGEN-Europe • European Energy Forum • AIoTI Relevant H2020 Projects • StoRIES

[102] https://www.ngiot.eu/event/ngiot-thematic-workshop-energy/?instance_id=146

5.3.2.5 Manufacturing

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

IoT and Edge Computing: Manufacturing[103]	
Current state, trends & opportunities	Challenges & barriers
Europe's **high-tech industry is declining** as biggest tech companies are located outside the EU. The manufacturing industry has a l**ow cloud adoption rate**, but Europe is **leading in industrial IoT** with high edge potential Edge offers a more **dynamic and efficient** environment with customized applications Security and privacy remain a concern	• **Lack of staff** with the right skills • Hierarchical silo organization in traditional industry • High investment **costs** • Secure data management • Connectivity outages • Legacy & IIoT infrastructure • **Key technical challenges** (Local AI model definition; 5G network controller • and TSN network controller interaction; Offloading compute capacity from AR glasses to Edge compute node).
Priorities and actions	Key organisations
Developing the glue between edge and cloud, through an open and secure architecture Investments in future employees/digital skills **Organisational change** for adopting and trusting edge and new business solutions Opening up for **partnerships, adopting open source and strengthening ecosystems**, including collaboration between large industry players and SMEs	• Artemis Industry Association • AIOTI • ROS Industrial Consortium • EFFRA • Productive 4.0 • AENEAS • EPoSS • IoT Forum

[103] https://www.ngiot.eu/event/ngiot-thematic-workshop-manufacturing/?instance_id=137

5.3.2.6 Automotive and Transportation:

Autonomous driving, predictive maintenance, traffic jams predictions, optimal route calculation and car tracking are one of the ways of utilization of IoT in the automotica and transportation industries which lead to greater efficiencies and cost savings. Mobility as a service also stands as a tremendous opportunity to create value in the public transport field[104].

IoT and Edge Computing: Automotive Industry[105]	
Current state, trends & opportunities	Challenges & barriers
The **transformation and fast growth** are driven by electrification and automation, associated with connected services for telematics, infotainment, and charging. The need for local awareness and real-time decisions **drive data to the edge**. While the American approach relies heavily on cameras, **European actors rely on sensors**. Sensor with **increasingly complex** data analysis and integration. Local computing power gives greater flexibility resulting in **less data sent to the cloud**, although many services will be connected to cloud facilities, at the same time. This requires new ways of **orchestration** to address data flows across the computing continuum (cloud – edge – IoT). Currently there is a widespread support of **standards like C-V2X, given Interoperability** of subsystems is crucial for the main functionalities. Edge offers opportunities for **real time** solutions, but the full potential of autonomous vehicles remains untapped, with European players at the vanguard, bringing new **HW opportunities**.	• Increased **complexity**, thus costly. **Reliability** is a challenge • **Interoperability** of subsystems in the cars • **Cross-border** service continuity • Security & Cybersecurity • **V2X** communications • Power & battery consumption • **Bandwidth** consumption
Priorities and actions	Key organisations
Move to **intelligent sensors. Integrate** car applications and sensor information. **Connectivity** up to the higher-level Edge infrastructure. Cloud infrastructure for **Over the Air** functionality updates. Move from HW applications to SW platforms. Faster **innovation cycles**. **Integration** with other sectors, such as energy. Partnerships and a strong **value network**	• ACEA • CLEPA • EATA • ERTRAC • ERTICO • C-Roads • CAR 2 CAR • 5GAA

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

[105] https://www.ngiot.eu/event/ngiot-thematic-workshop-automotive-industries-and-mobility/?instance_id=149

5.3.2.7 Insurance and Finance

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

IoT and Edge Computing: Insurance and Finance	
Current state, trends & opportunities	Challenges & barriers
Deployment of IoT in the insurance industry has benefitted mostly underwriting and claims[106]. Insurers with IoT knowledge deliver greater value by offering new services and cross-industry products, and manage reduce fraud by leveraging data to analyze each particular case. The finance industry has leveraged IoT in many ways, particularly in the widespread adoption of cards and other smart payment methods.	• Susceptibility of devices and networks • Trust - IoT devices are not protected by design. No standard of compliance to safeguard devices[107] • Hardware failure • Investment in infrastructure and data • Cyber risk and data privacy • Connected networks at scale
Priorities and actions	Key organisations
Establishing customer buy-in and trust Facilitate adoption and overcome transformational challenges Data privacy and security by desing	• EBF • CBI • IMIA Relevant H2020 projects • FINSEC • INFINITECH

[106] https://www.capgemini.com/wp-content/uploads/2020/05/IoT-Insurance-of-Things-1.pdf

[107] https://cyberstartupobservatory.com/the-bank-of-things-the-application-of-iot-in-the-financial-sector/

6 CONCLUSIONS AND FUTURE STEPS

6.1 Timelines: from research to mature solutions

In the previous section we identified research, innovation and deployment priorities according to our analysis. To analyse the maturity of research in the above topics and hence define their evolution in the next future we leveraged on the insights from different sources including IoT Analytics[108], Gartner[109], ARTEMIS-IA[110], ATOS and stakeholders feedbacks.

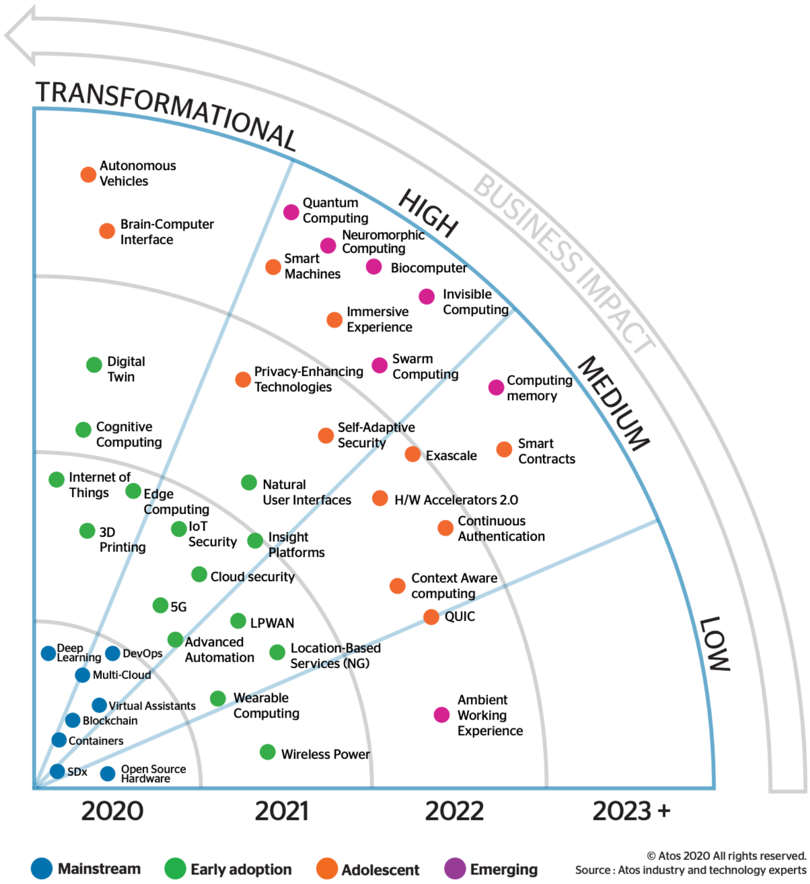

Figure 29. Atos Tech Trends Radar 2021[111]

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

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

[110] AENEAS, ARTEMIS-IA and EPoSS. ECS Strategic Research Agenda 2021 (2021)

[111] ATOS. Tech Trends Radar (2021).

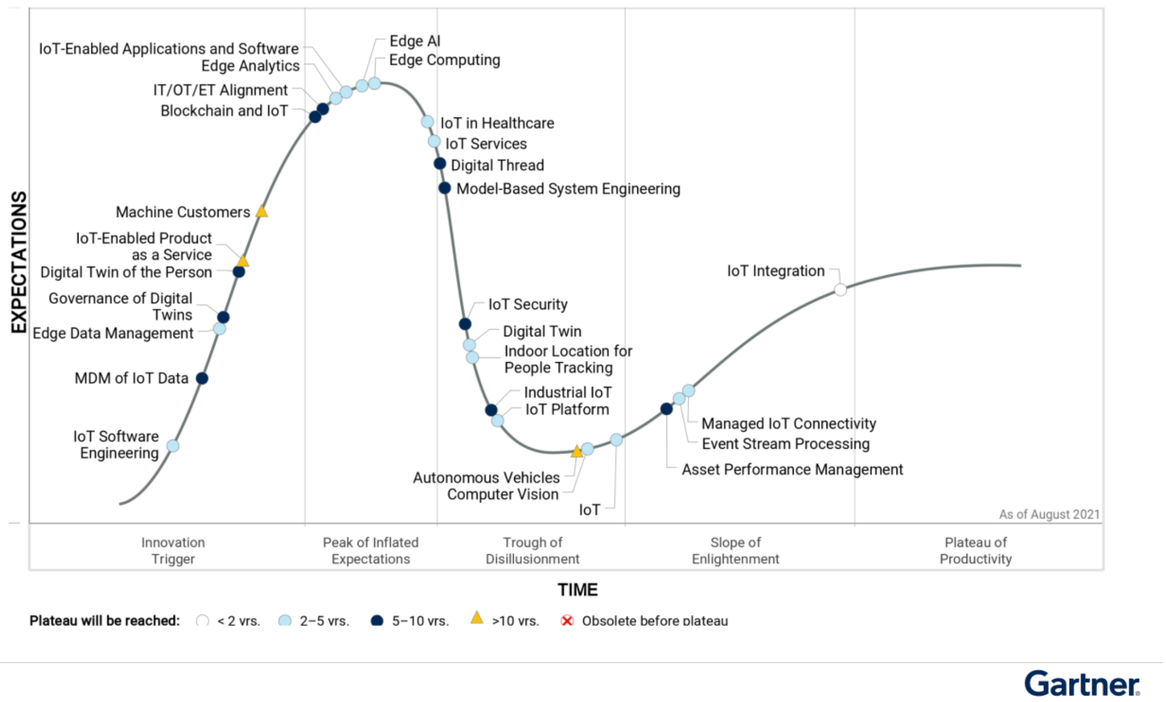

Figure 30. Hype Cycle for the Internet of Things, Gartner, 2021[112]

[112] Gartner. Hype Cycle for the Internet of Things (2021)

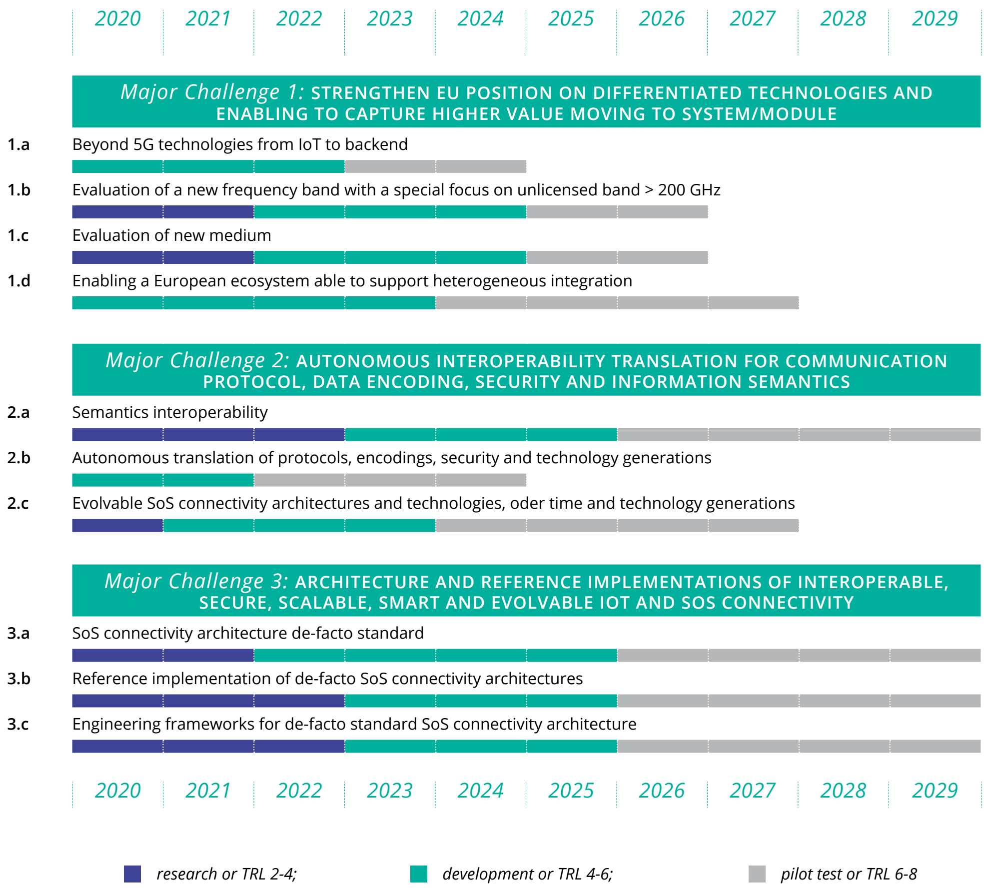

Figure 31. ECS Challenges time frame for Connectivity and Interoperability[113]

Table 3 presents the timeline of R&I&D priorities over the period 2022-2030 highlighting the expected maturity: research or TRL 2-4 ( ), technology development and field test or TRL 4-6 ( ) and pilot tests or TRL 6-8 ( ). The table also reports the key technology enablers for each of the priorities. Timeframe has been selected taking into consideration the scope of the upcoming work programmes part of the new MFF. Obviously, taking into consideration the rapid evolution of digital technologies, the medium-term (2024-2025) and longer term (2025-2030) timelines will require additional updates and reassessments in the future.

[113] AENEAS, ARTEMIS-IA and EPoSS. ECS Strategic Research Agenda 2021 (2021)

Table 3. R&I&D priorities timeline for IoT over the period 2022-2030.

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

	Timeline						
Research topic	2022	2023	2024	2025	2026	2027	>
R-IOT1.1 Large IoT & digital infrastructures							
R-IOT.1.2 Autonomous IoT infrastructures							
R-IOT.2.1 Sustainable IoT by design							
R-IOT.2.2 Augmented IoT							
R-IOT.2.3 Tactile Internet							
R-IOT.2.4 IoT for sustainability							
R-NET.1.1 Low-cost, high-volume connectivity							
R-NET.1.2 Low-power connectivity schemes							
R-DATA.1.1 Highly scalable and low latency ledgers for IoT							
R-DATA.1.2 Unified processing paradigm							
R-DATA.2.1 MLOps and decentralised AI/ML pipelines							
R-DATA.2.2 Lightweight AI and ML							
R-DATA.2.3 From federated machine learning and swarm learning							
R-DATA.3.1 AI for Humans: understandable and ethical decisions							
R-DATA.3.2 Validated AI algorithms for IoT use cases							
R-DATA.4.1 IoT data dictionaries deployed at scale							
R-DATA.4.2 Semi-automated data interoperability							
R-DATA.4.3 Semi-automated process interoperability							

	Timeline						
Research topic	2022	2023	2024	2025	2026	2027	>
R-DATA.5.1 IoT data market architectures							
R-DATA.5.2 Novel business models to incentivise data sharing							
R-DATA.5.3 Large data marketplaces for IoT scenarios							
R-CLOUD.1 Self-* for edge computing							
R-CLOUD.2 From centralised orchestration to collaborative orchestration							
R-CLOUD.3 Energy aware cloud-to-edge infrastructures							
R-ELET.1.1 Energy efficient devices							
R-ELET.1.2 Sustainable devices							
R-ELET.2 Native AI-capable edge devices							
R-SEC.1.1 AI-powered cybersecurity							
R-SEC.1.2 Data traceability and trust in the cloud-edge era							
R-SEC.2.1 Privacy-by-design for IoT devices							
R-SEC.2.2 Security & Privacy-by-design for IoT services							

6.2 Recommendations for the Horizon Europe programme

6.2.1.1 Data value

Sustain activities around data value in the relevant work programmes, **increasing focus on IoT generated data** covering architectures (R-DATA.5.1 - IA) and business models (R-DATA.5.2 - RIA) **and** boost research on **novel solutions for data processing** using IoT as a primary data source, **both at the software** (R-DATA.1.2 - RIA) **and hardware stacks** (R-ELET.2 - RIA). In the short term research should focus on enabling distributed/decentralised AI and ML tasks leveraging today's state of the art: i.e., supporting distributed / decentralised AI pipelines and AI model training, while increasing through devops approaches the level of automation. In the short-medium term, research should focus on novel approaches to reduce computational requirements of computing and executing AI algorithms. In the longer term, research should look into disruptive approaches that will handle barriers of today architectures. This research is instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

6.2.1.2 IoT Networks

Foster research in the Future Network area that will ensure the development of **reliable, low-cost and scalable IoT networks** (R-NET.1.1 - RIA) and **reduce energy impact of IoT networks** (R-NET.1.2 / R-ELET.1.1 / R-CLOUD.3 - RIA). Support further **experimentation and deployments** of the next generation of reliable, low-cost and scalable IoT networks, opening the paths to achieve the convergence of processing and data transfer in the long term future (R-DATA.1.2 - RIA).

6.2.1.3 Foster cost-efficiency of solutions

Focus on the increase of automation to **reduce the cost of the management of complex IoT platforms and networks** applying at scale automatic approaches (R-IOT.1.2 / R-CLOUD.1 / R-CLOUD.2 - RIA) to govern IoT infrastructures, while researching semi-automatic approaches for data (R-DATA.4.2 - RIA), and process interoperability (R-DATA.4.3 - RIA).

6.2.1.4 Data Management

Focus on the **transition from data management to insight generation from data** by delivering ready-to-use AI algorithms in different scenarios (R-DATA.3.2 - IA), on the increase of automation **to reduce the cost of the management of complex IoT platforms** and networks focusing on semi-automatic approaches as a first step (R-IOT.1.2 - RIA / R-CLOUD.1 / R-CLOUD.2 / R-DATA.4.2 - RIA) and enabling unified data processing from cloud servers to embedded processing units (R-DATA.1.2 - RIA).

6.2.1.5 IoT / Edge Operating Systems

Go beyond "meta" Operating Systems. ROS are quite mature examples of "meta" operating systems, although they lack integration of dev-ops approaches, and other characteristics of modern cloud native technologies. The real challenge today to enable the cloud-edge continuum, is in the scalable distributed/decentralised management of resources and services and their optimization in the cloud-edge continuum to comply with different functional and non-functional requirements. In this respect, the short term research should focus on **semi-autonomous orchestration (**R-CLOUD.1) and coordination mechanisms on top of abstraction layers that simplify the interaction with heterogeneous resources **(**R-CLOUD.2). In the longer term, **AI may increase the levels of autonomy** and facilitate the move from centralised orchestration towards decentralised coordination.

6.2.1.6 IoT integration with other technologies

Leverage the advancements in Artificial Intelligence, Distributed Ledgers and other technologies to evolve IoT platforms beyond today's limitations by introducing dynamic orchestration of AI processes (R-DATA.2.1 - RIA), making AI decisions human understandable (R-DATA.3.1 - RIA), increasing scalability and reducing latency of distributed ledgers (R-DATA.1.1 - RIA). As the emphasis on AI and hardware convergence is increased, the untapped potential will be closer to the edge while ensuring energy efficiency.

Further down the road, IoT platforms should evolve by introducing **dynamic orchestration of AI processes at large scale** (R-DATA.2.1 - IA). However, with major microprocessor producers being located outside Europe, it is essential to increase the EU capacity on this front with focus on AI, rather than dispersing resources on multiple areas of specialisation. In the longer term the focus should be on bringing neuromorphic computing based PU to the market.

6.2.1.7 Machine-human interaction

Prioritise the research on **machine-human** interaction in the IoT arena **following a multidisciplinary approach** by scouting solutions for extended reality, including augmented reality, and digital twins (R-IOT.2.2 - IA), tactile internet (R-IOT.2.3 - IA), while targeting a sustainable IoT by design (R-IOT.2.1 - RIA).

6.2.1.8 IoT trials

Support large deployments of standard and replicable solutions, establishing IoT trials in new domains beyond the ones covered today by the IoT Large Scale Pilots[114] (LSPs), such as Energy Management, Insurance (IA) and Media, Transportation, and Safety & Defence (RIA). In several domains, IoT deployments are still at the level of proof of concepts. The lack of large scale deployments is clearly limiting the understanding of requirements to support such deployments in different domains. These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

Invest and leverage on experimental infrastructures to support testing and experimentation of cloud-edge solutions. Developing and testing cloud-edge solutions is clearly more complex than testing solutions for the cloud, or on premises. The lack of availability of infrastructures supporting experimentation in the "continuum" may clearly slow down the development and testing of solutions, especially by small players such as SMEs. It is important to build such capacity in the short term, and to maintain it in the longer one, to ensure that EU innovators can be sustained in the access to cloud-edge playgrounds to build, test, and scale their products.

In this context, the research programme should encourage future funded projects to use of European research infrastructures supported by ESFRI, including SLICES which is developing a European large scale research and test infrastructure for information and communication technologies, encompassing IoT, edge computing and coud, including network and system virtualization.

6.2.1.9 Research future-proof security and privacy by design

Develop security-by-design and privacy-by-design IoT architectures and technologies (R-SEC.2.2 - RIA) capable of dealing with future threats (R-SEC.1.1 - RIA) and increasing traceability and trust of IoT generated data (R-SEC.1.2 - IA). Beyond regulatory compliance with the GDPR, ePrivacy and NIS Directive, there is a high potential for innovation in data protection by design technologies for the IoT, edge and cloud continuum, including networking technologies. Such technologies will be instrumental to enable the development of the European Data strategy and Digital Single Market. It will also enable to address a growing demand for privacy compliant solutions in all countries that have adopted data protection regulations.

6.2.1.10 Green and sustainable IoT

Develop **IoT miniaturisation** (R-ELET.2 - RIA), **energy harvesting** (R-ELET.1.1 - RIA) **and pervasiveness** while **ensuring the environment compatibility** (R-ELET.1.2 - RIA) of this new generation of devices. The relevance of IoT supporting sustainability goals must be highlighted. While low-power processing and energy efficient data processing are surely essential to ensure sustainability of IoT solutions, more needs to be done in this regarding the whole lifecycle of IoT products, making them more environmentally compatible and cheaper to deploy, connect and operate. Research in the longer term should focus on easy to recycle, longer lasting, and more environmentally compatible devices. In the shorter term, research

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

should increase the spectrum of scenarios where IoT is explored as a way to improve sustainability and environmental friendliness of devices.

6.2.1.11 IPR protection and patent promotion

Enhancing **IPR and marketing support** for future European research projects on IoT, by providing complementary funding for covering **IPR protection costs related to IoT research and innovation results**. Linked to this, it is recommended that the next research programme on IoT encourage research projects to **apply for patents**. The programme could also request that patents, if not exploited by the applicant, should be licensed to European industries within a delay of 12 months. However, this implicates dedicated financial and technical support with experts made freely available to help researchers in redacting and filling patents to protect IoT research and development results financed by the EC.

6.2.1.12 Project impact promotion and assessment

Increase the impact of the relevant call related to IoT and Edge computing by adapting the process for reducing the **time-to-market from research project application to marketable products and services**. The programmes should increase the focus of the calls on IoT to adapt to market needs, create more momentum and stimulate a global and dynamic approach. We recommend involving an evaluator in the mid-term review of a research project to assess its exploitation potential and provide guidelines and orientations on possible funding. A post-project assessment is also encouraged, one year after the end of the project, to follow up on its results and its impact. As a point of comparison, digital developments in Asia and the United States raise expectations of highly customised products and services at a rapid rate that challenge European companies to innovate more effectively, making them lag, caught between high costs, legacy ecosystems, and ageing workforces[115].

6.2.1.13 Cascade funding

The research and innovation programme is not always easily accessible to newcomers and, in particular, to SMEs and start-ups. Cascade funding is considered a good practice that should be further encouraged. It was identified by several Strategy Board members as an efficient mechanism to attract and include SMEs in the European research activities. We recommend encouraging the use of cascade funding in IoT, Edge, Cloud calls for proposals in order to engage with new companies, SMEs and start-ups. Similarly, the active participation of IoT-related SMEs and start-ups should be encouraged.

6.3 Recommendations for the Digital Europe programme

6.3.1.1 Secure and Ethical IoT

Support initiatives aimed at increasing **trust in IoT adoption** through **cybersecurity and privacy-by-design** (GDPR compliance), as well as those seeking a better understanding of **ethics and privacy** implications by deploying at large scale state-of-the art solutions for IoT services cyber-security (R-SEC.2.2). These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

[115] Deloitte. 'Innovation in Europe'. Accessed 15 May 2021. deloitte.com/

6.3.1.2 Data models for interoperability and replicability

Sustain the **development and uptake of cross-domain harmonised data models**, following the path established by OASC with the MIMs[116], to **increase IoT application interoperability and replicability** especially in the public sector across Europe (R-DATA.4.1), fostering them as requirements in related public procurements. Following this development, a key driver is the Smart Data Models initiative led by FIWARE, IUDX, TM Forum, OASC and other organisations to support the adoption of common compatible data models in smart solutions[117]. These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

6.3.1.3 Innovation transfer

Transfer the experience matured by running LSPs in the sectors of Smart Cities, Agriculture and Healthcare to a wider set of actors **through joined innovation procurement** and similar actions. The success of the LSPs needs to be scaled up by making these experiences widespread. Although this recommendation faces big hurdles, like lack of trust, replicability, scalability and support to SMEs and start-ups to achieve a wider expansion of the solutions, these activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

6.3.1.4 Scalability

Deploy secure and highly scalable IoT and digital infrastructures (R-IOT1.1) with special focus on edge capacity, leveraging on global networking technologies such as IPv6 and 5G. These activities are instrumental for the realisation of EU Data Spaces as envisioned in the EU Data Strategy.

6.3.1.5 Sustainability

Leverage the potential of IoT for sustainable development, in line with the UN Sustainable Development Goals (SDGs) (R-IOT.2.4). The Green Deal and SDGs constitute an important opportunity to develop innovative technologies aligned with societal needs and demands. We recommend having dedicated calls for proposals for IoT, Edge, Cloud with a focus on Sustainable Development Goals and the Green Deal.

6.3.1.6 Independence and sovereignty

Contribute to the technological independence and autonomy of Europe in terms of IoT critical infrastructures and services by increasing the scale of IoT infrastructure available to EU citizens (R-IOT1.1) leveraging common and free access to data standards (R-DATA.4.1) and providing secure-by-design IoT services (R-SEC.2.2). The European landscape has strong SMEs capable of developing solutions across the different segments that comprise the IoT and Edge computing fields, giving it the capability of reaching a certain degree of technological independence and autonomy.

6.3.1.7 IoT Skills Development

Although the lack of digital skill and talent retention has been a common point of preoccupation across several of the research methods and activities, it can only be reflected in the recommendation of Innovation transfer. Strengthening the digital skill across the IoT and Edge computing-related fields (E3) to be applied across vertical domains is one of the necessary pieces to be in place to unfold the full potential of these technologies. Europe's strong academic

---

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

[117] https://github.com/smart-data-models

landscape and journal publications need to be further aligned with industry needs and play on the advantages of having an excellent quality of live and active research communities to foster talent retention versus other latitudes that play on the economic retribution and renown of working for a global tech leader. Developing (Upskilling) and keeping (Reskilling) the right talent is key to increase European influence in the global tech landscape whilst taking the lead in niche areas to keep at bay the competition from Asia and America.

6.3.1.8 Open Innovation

Develop open source IoT/Edge platforms that are more ubiquitous, pervasive, scalable, autonomous, light and sustainable (S4). New research projects should use/extend/adapt existing open source platforms when they already exist.

Re-starting a new open source platform from scratch should be motivated by positioning this new open source platform regarding to the existing ones, and explaining why this new platform is needed and why the requirements it covers can not be addressed by contributing or extending an existing platform This approach will enable the creation of research platforms that are sustainable, reused and extended by the contribution of several complementary research projects and that have more chances of being adopted by the industry.

Research projects should involve experts in these domains, either independent, or affiliated to an open source foundation, to avoid the pitfalls of a naive approach of open source. Doing proper open source is more than publishing code: Open Source governance, Open Source IP management, and community development require significant expertise and effort.

Invest in training and education for implementing open source platforms to strengthen the European open source ecosystem and foster uptake of open source strategies/business models. This should be integrated deeply into the European research agenda.

6.3.1.9 Cooperation and standardisation

To enhance the cooperation among all IoT related organisations and fora to maximise the synergies among them, to reduce the fragmentation of the European IoT community, and to increase harmonisation of IoT cloud-edge standards. The IoT Market will be shaped by global standards. As of today, there are a number of competing initiatives around cloud-edge. While many of them are based on open source, they enforce different "standards" to realise cloud-edge (for IoT), thus increasing the risk of fragmentation and leading to potential interoperability issues. Before the proliferation of standards and open source solutions becomes an actual brake on adoption, it is important to support the harmonisation of existing standards and open solutions. In order to maximise the direct impact of the standardisation work at an international level and also to reduce the time-to-market of a standard, we encourage direct contribution to global standardisation processes led by global SDOs such as IEEE, IETF, ITU, ISO, IEC, 3GPP and TM Forum as well as the development of best practices through industrial alliances and open-source communities.

6.3.1.10 Large-scale research infrastructure

Research on IoT, Edge, Cloud requires to access adequate research infrastructure able to research, test, and validate the interoperability and scalability of innovative technologies. In order for Europe to remain competitive in this domain, leveraging and synergising with existing infrastructure to develop a European-wide research infrastructure for IoT, Edge, Cloud is perceived of paramount importance to enable the European research and innovation programme to research and develop the technologies and solutions that will shape the future Internet infrastructure. In order to succeed on the market, research projects should research and develop technologies that are interoperable and scalable by design. Leveraging large scale research infrastructures (i.e., SLICES, Fed4FIRE+, etc.) and scalable platforms (i.e., GAIA-X, FIWARE, etc.) should be considered by projects.

6.4 Recommendations for the Connecting Europe Facility 2 programme

6.4.1.1 Large band connectivity across digital infrastructures

Facilitate access to large computational facilities needed to harness the complexity of analysing terabytes (or petabytes) of IoT generated data and ensure sovereignty by deploying digital infrastructures across Europe (R-IOT1.1) that are interconnected with high speed internet. These activities are instrumental for the realisation of EU Data Spaces and Federated Clouds as envisioned in the EU Data Strategy.

7 REFERENCES

5G-ACIA. (2021). *5G ACIA Testbeds*. Retrieved from https://5g-acia.org/testbeds/

ABI Research. (2019). Digital Twins, Smart Cities, and Urban Modeling. Retrieved from https://www.abiresearch.com/market-research/product/1033835-digital-twins-smart-cities-and-urban-model/

ACEA. (2021). *Chip shortage: auto industry calls for more EU-made semiconductors.* Retrieved from https://www.acea.auto/message-dg/chip-shortage-auto-industry-calls-for-more-eu-made-semiconductors/

Aeneas, Artemis & EpoSS. (2020). ECS Strategic Research Agenda (ECS-SRIA) 2020. https://www.ngiot.eu/wp-content/uploads/sites/73/2020/09/ECS-SRA-2020.pdf

Aeneas, Artemis & EpoSS. (2021). ECS Strategic Research and Innovation Agenda (ECS-SRIA) for Electronic components and Systems. https://aeneas-office.org/wp-content/uploads/2021/01/2021_ECS-SRIA-final_1501.pdf

AENEAS, Artemis IA, EPoSS. (2021). *Strategic Research and Innovation Agenda 2021.* Berlin, Germany.

AENEAS, ARTEMIS-IA & EPoSS. (2020). *ECS Strategic Agenda 2020.* Retrieved from https://artemis-ia.eu/publication/download/ecs-sra-2020.pdf

AER. (2020). *Brain Drain vs Brain Gain.* Retrieved from https://aer.eu/brain-drain/

AIOTI. (2019). *IoT Relation and Impact on 5G*. Retrieved from https://aioti.eu/wp-content/uploads/2019/03/AIOTI-IoT-relation-and-impact-on-5G-190308-R2-published.pdf

AIOTI. (2020). *HLA*. Retrieved from https://aioti.eu/wp-content/uploads/2020/12/AIOTI_HLA_R5_201221_Published.pdf

AIOTI. (2020). *IoT data marketplaces for the agri-food sector: a first look to use cases for smart farming and across the food chain.* Retrieved from https://aioti.eu/wp-content/uploads/2020/05/AIOTI-WG06-IoT-data-markets-agrifood-v1.pdf

Alliance of Internet of Things Innovation, InnoEnergy, ENTSO-E, SDA Bocconi. (2021). White Paper - Open Energy Marketplaces evolution: Beyond Enabling Technologies. https://aioti.eu/wp-content/uploads/2021/03/Open-Energy-Marketplaces-Evolution- Published.pdf

Annicchino, P., Brékine, A., Facca, F.M., Heijnen, A., & Castro, F.M. (2018). IoT research, innovation and deployment priorities in the EU White Paper. NGIoT. https://www.ngiot.eu/wp-content/uploads/sites/26/2020/09/D3.1.pdf

Annicchino, P., Cappparelli F., Audino, A., Rosignuolo, G., Landi, A., & Seminara, S. (2018). Privacy, Security and Trusted IoT Observatory Report. NGIoT. Retrieved from https://cordis.europa.eu/project/id/825082/results

Artemis Industry Association. (2020, April). From Internet of Things to System of Systems: Market analysis, achievements, positioning and future vision of the ECS community on IoT and SoS - An ARTEMIS-IA Whitepaper. https://www.eurotech.com/attachment/download?id=2094

Ashton, K. (2009). That 'internet of things' thing. *RFID Journal*, 22.7.

AT Kearney. (2016). *IoT: A new path to European prosperity*. Retrieved from https://www.kearney.com/digital/article?/a/the-internet-of-things-a-new-path-to-european-prosperity

ATOS. (2018). *Swarm Computing Concepts, technologies and architecture.*

Atos. (2020). What the world will look like after the COVID-19 crisis. https://atos.net/content/2020/atos-report-what-the-world-will-look-like-after-the-covid-19-crisis.pdf

ATOS. (2021). *Which technologies will power your business tomorrow?* Retrieved from https://atos.net/en/lp/lookout-industry-trends/tech-trends-radar

Bain & Company. (2018). *Europeans Extend Their Lead in the Industrial Internet of Things.* Retrieved from https://www.bain.com/contentassets/325cb60011ee4cbd8891381ec5ed781e/bain_brief_europeans_extend_their_lead_in_the_industrial_iot.pdf

Bain & Company. (2018). *Unlocking opportunities in the IoT.* Retrieved from https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things/

Bain & Company. (2020). Technology Report 2020: Taming the Flux. https://www.bain.com/globalassets/noindex/2020/bain_report_technology-report-2020.pdf

Bauer, M. (2013). IoT reference architecture. *Enabling Things to Talk*, 163-211.

Bisson, R. (2021). *Horizon Europe 'bureaucracy' a fear in Australia and New Zealand*. Retrieved from https://www.researchprofessionalnews.com/rr-news-europe-horizon-2020-2021-8-horizon-europe-bureaucracy-a-fear-in-australia-and-new-zealand/

Bravo, C., & Bäckstöm, H. (2020). Edge computing and deployment strategies for communication service providers. Ericsson. Retrieved from https://www.ericsson.com/en/reports-and-papers/white-papers/edge-computing-and-deployment-strategies-for-communication-service- providers

Brynskov, M. (2021). Virtualisation Taking Place. Lecture to the European Commission CONNECT University. https://futurium.ec.europa.eu/en/connect-university/events/digital-solutions-climate-change-mitigation-and-adaptation-cities-and-communities

Brynskov, M., Facca, F.M., & Annicchino, P. (Eds). (2020). Preliminary Roadmap for IoT Research, Innovation and Deployment in Europe. NGIoT. Retrieved from https://www.ngiot.eu/resources/publications/

Brynskov, M., Facca, M.F., Hrasko, G. (Eds). (2019). Building a Roadmap for the Next Generation Internet of Things: Research, Innovation and Implementation 2021-2027. NGIoT. https://www.ngiot.eu/wp-content/uploads/sites/73/2019/09/NGIoT_scoping-paper.pdf

Carvalho, L.I, da Silva, D.M.A., Sofia, R.C (2020, March 12). Leveraging Context-awareness to Better Support the IoT Cloud-Edge Continuum. In Proc. of The Fifth International Conference on Fog and Mobile Edge Computing (FMEC 2020) Paris, France. Retrieved from https://easychair.org/publications/preprint/ckDL

CBI. (2021). *The European market potential for (Industrial) Internet of Things.* Retrieved from https://www.cbi.eu/market-information/outsourcing-itobpo/industrial-internet-things/market-potential

CEMA. (2020). *Full deployment of agricultural machinery data-sharing: technical challenges & solutions.* Retrieved from https://cema-agri.org/images/publications/position-papers/2020_02_05_CEMA_PT3_PP_Strategy_paper_agricultural_machinery_data_sharing.pdf

Chabas, J.M., Gnanasambandam, C., Gupte, S., & Mahdavian, M. (2018, November 8). New demand, new markets: What edge computing means for hardware companies. McKinsey & Company. Retrieved from https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/new-demand-new-markets-what-edge-computing-means-for- hardware-companies#

ClimateLaunchpad. (2020). *The European Green Deal Offers Massive Opportunities For Green Business.* Retrieved from https://climatelaunchpad.org/the-european-green-deal-offers-massive-opportunities-for-green-business/

CNBC. (2019). *Here are the 5 biggest beneficiaries of the 5G rollout: Jim Cramer*. Retrieved from https://www.cnbc.com/2019/02/06/cramer-here-are-the-5-biggest-beneficiaries-of-the-5g-rollout.html

Commision, E. (2021). *Europe's Internet of Things Policy.* Retrieved from https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy

Control engineering. (2020). *2020 SYSTEM INTEGRATOR GIANTS.* Retrieved from https://www.controleng.com/events-and-awards/system-integrator-giants/2020-system-integrator-giants/

D'Acquisto, G. e. (2015). *Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics.*

DECISION Etudes & Conseil. (2020). *Study on Emerging Technologies in Electronic Components and Systems (ECS) – Opportunities ahead.* Retrieved from https://wayback.archive-it.org/12090/3/https://ec.europa.eu/digital-single-market/en/news/emerging-technologies-electronic-components-and-systems-ecs-opportunities-ahead-0

Deloitte. (2020). *The fourth industrial revolution.* Retrieved from https://www2.deloitte.com/content/dam/insights/us/articles/us32959-industry-4-0/DI_Industry4.0.pdf

DIGIBYTE. (2021). *Digital Skills and Jobs Platform: the one-stop-shop to close Europe's digital skills gap.* Retrieved from https://digital-strategy.ec.europa.eu/en/news/digital-skills-and-jobs-platform-one-stop-shop-close-europes-digital-skills-gap

DIGITAL SME. (2020). *DIGITAL SME input on the EC's White Paper on Artificial Intelligence (AI)*. Retrieved from https://www.digitalsme.eu/digital/uploads/DIGITAL-SME-Position-Paper-AI-White-Paper_FINAL-1.pdf

Dorofeev, K., Walzel, H., & Sofia., R.C. (2021). Brownfield Devices in industrial Internet of Things - Automating the Integration via Semantic Technologies. Fortiss. https://www.fortiss.org/fileadmin/user_upload/05_Veroeffentlichungen/Informationsmateri ali en/fortiss_whitepaper_Brownfield_devices_in_IIoT_web.pdf

DW. (2011). *Language barrier limits European Internet users, study shows.* Retrieved from https://www.dw.com/en/language-barrier-limits-european-internet-users-study-shows/a-15067034-1

Earls, A. (2019). *IoT Readiness: Is Europe up to it?* Retrieved from https://www.smart-industry.net/iot-readiness-is-europe-up-to-it/

EC, European Commission. (2019). Rethinking strategic autonomy in the digital age. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/889dd7b7-0cde-11ea-8c1f-01aa75ed71a1/language-en/format-PDF/source-118121846

EC, European Commission. (2019). What is the European Green Deal? Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/fs_19_6714

EC, European Commission. (2020). A Europe Fit for the Digital Age. Retrieved from https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en#latest

EC, European Commission. (2020). COMMUNICATION. A European Strategy for Data. https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb2020_en.pdf

EC, European Commission. (2020). COMMUNICATION. A New Industrial Strategy for Europe. https://ec.europa.eu/info/sites/default/files/communication-eu-industrial-strategy-march-2020_en.pdf

EC, European Commission. (2020). COMMUNICATION. An SME Strategy for a sustainable and digital Europe. https://ec.europa.eu/info/sites/default/files/communication-sme-strategy- march-2020_en.pdf

EC, European Commission. (2020). Data Governance Act. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

EC, European Commission. (2020). Supporting the green transition. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/FS_20_281

EC, European Commission. (2020). WHITE PAPER. On Artificial Intelligence - A European approach to excellence and trust. https://ec.europa.eu/info/sites/default/files/commission- white-paper-artificial-intelligence-feb2020_en.pdf

EC, European Commission. (2021). Coordinated Plan on Artificial Intelligence 2021 Review. Retrieved from https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

EC, European Commission. (2021). Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983

Eclipse Foundation. (2019). IoT Commercial Adoption Survey 2019 Results. Retrieved from https://outreach.eclipse.foundation/iot-adoption-2019

Eclipse Foundation. (2020). Enabling Digital Transformation in Europe Through Global Open Source Collaboration. https://www.eclipse.org/europe/documents/eu-opensource-whitepaper-jan2021.pdf

Eclipse IoT. (n.d). Open Source for IoT. Retrieved from https://iot.eclipse.org/

Edge Native. (n.d.). Edge Native Working Group. Retrieved from https://edgenative.eclipse.org/

EdgeIR. (2021). *Edge Computing Companies*. Retrieved from https://www.edgeir.com/edge-computing-companies

EETimes. (2019). *European Consortium to Develop Standard Edge Computing Platform.* Retrieved from https://www.eetimes.com/european-consortium-to-develop-standard-edge-computing-platform/

ENISA. (2020). *2020 main incidents.* Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents

ENISA. (2020). *ENISA Threat Landscape 2020.* Retrieved from https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

EPEC. (2021). *European PPP Expertise Centre*. Retrieved from https://www.eib.org/epec/

Ericsson. (2018). *Ericsson Mobility Report.* Retrieved from Ericsson: https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-june-2018.pdf

Ericsson. (2020). *Edge computing and deployment strategies for communication service providers.* Retrieved from https://www.ericsson.com/en/reports-and-papers/white-papers/edge-computing-and-deployment-strategies-for-communication-service-providers

Ericsson. (2021). *Ericsson named a Leader in the 2021 Gartner Magic Quadrant for 5G Network Infrastructure for Communications Service Providers report*. Retrieved from https://www.ericsson.com/en/press-releases/2021/2/ericsson-named-a-leader-in-the-2021-gartner-magic-quadrant-for-5g-network-infrastructure-for-communications-service-providers-report

EU LSP Programme. (2018). Retrieved from IoT Pilot Architecture: https://european-iot-pilots.eu/architecture-analysis/

EuChems. (2019). *EU Research and Development Directorate-General attempts to tackle bureaucratic functioning.* Retrieved from https://www.euchems.eu/newsletters/eu-research-and-development-directorate-general-attempts-to-tackle-bureaucratic-functioning/

Euraxess. (2016). *The manufacturing Sector in Europe*. Retrieved from https://cdn4.euraxess.org/sites/default/files/labor_market_information-_manufacturing_sector.pdf

European Comission. (2021, May). *Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy.* Retrieved from https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and

European Commision. (2021). *Entrepreneurship and small and medium-sized enterprises (SMEs)* . Retrieved from https://ec.europa.eu/growth/smes_en

European Commision. (2021). *Europe's Internet of Things Policy*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy

European Commission . (2020). *Automotive Industry*. Retrieved from https://ec.europa.eu/growth/sectors/automotive-industry_en

European Commission. (2018). *The European AI Landscape*. Retrieved from https://knowledge4policy.ec.europa.eu/publication/european-ai-landscape_en

European Commission. (2019). *THE NEXT EU RESEARCH & INNOVATION INVESTMENT PROGRAMME (2021 – 2027).* Retrieved from https://ec.europa.eu/info/sites/default/files/research_and_innovation/strategy_on_research_and_innovation/presentations/horizon_europe_en_investing_to_shape_our_future.pdf

European Commission. (2020). *Horizon 2020 - Work Programme 2018-2020. Information and Communication Technologies.* Retrieved from https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-leit-ict_en.pdf

European Commission. (2021). *European Alliance for Industrial Data, Edge and Cloud* . Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance

European Commission. (2021). Retrieved from https://smart-cities-marketplace.ec.europa.eu/

European court of auditors. (2018). *Public Private Partnerships in the EU*. Retrieved from https://www.eca.europa.eu/Lists/ECADocuments/SR18_09/SR_PPP_EN.pdf

European Fundraising Association. (2021). *Insights into digital adoption across Europe revealed in global report*. Retrieved from https://efa-net.eu/news/insights-digital-adoption-europe-revealed-global-report

European Investment Bank. (2020). *Accelerating the 5G transition in Europe*. Retrieved from https://www.eib.org/attachments/thematic/accelerating_the_5g_transition_in_europe_en.pdf

European Parliament. (2014). *Mapping Smart Cities in Europe.* Retrieved from https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf

eurostat. (2020). Retrieved from Proportion of ICT specialists in total employment: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment

Ferrando, A., Lekpek, S., & Veugele, R. (2019). Young SMEs as a Motor of Europe's Innovation Machine. *Intereconomics*, 369-377.

Ferrer, A.J., Iorizzo, C., Staarink, J., Gruber, M., Pichler, W., Kurstjens, P., & Janezcko, J. (2018). Swarm computing. Computing concepts, technologies and architectures. Atos Whitepaper. https://atos.net/wp-content/uploads/2018/12/atos-swarm-computing-white-paper.pdf?utm_source=LP

FICCI & EY India (2019). Future of IoT. FICCI. https://ficci.in/spdocument/23092/Future-of- IoT.pdf

FICCI & EY. (2019). *Future of IoT.* Retrieved from https://ficci.in/spdocument/23092/Future-of-IoT.pdf

Fireside Chat of 9 March 2021 European Commission, CNECT-E4 31 March 2021, Event report. Retrieved from: https://ec.europa.eu/newsroom/dae/redirection/item/707669

FIWARE. (2020). Retrieved from https://www.fiware.org/developers/catalogue/

Forrest, C. (2018). *ZDNET*. Retrieved from https://www.zdnet.com/article/10-edge-computing-vendors-to-watch/

Fremantle, P. (2015). *A Reference Architecture For The Internet of Things*. Retrieved from WSO2: https://wso2.com/whitepapers/a-reference-architecture-for-the-internet-of-things/

Gartner. (2019). *Gartner Says Worldwide IaaS Public Cloud Services Market Grew 31.3% in 2018*. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2019-07-29-gartner-says-worldwide-iaas-public-cloud-services-market-grew-31point3-percent-in-2018

Gartner. (2019). *Magic Quadrant for Industrial IoT Platforms.* Retrieved from https://b2bsalescafe.files.wordpress.com/2019/09/gartner-magic-quadrant-for-industrial-iot-platforms-june-2019.pdf

GDPR. (2016a). Art. 4. Retrieved from https://gdpr.eu/article-4-definitions/

GSMA. (2019). *Internet of Things in the 5G Era.* Retrieved from https://www.gsma.com/iot/wp-content/uploads/2019/11/201911-GSMA-IoT-Report-IoT-in-the-5G-Era.pdf

Hobbs, C. (2020). *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry.* Retrieved from https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/

Hüttenrauch, M. A. (2019). Deep reinforcement learning for swarm systems. *Journal of Machine Learning Research 20(54)*, 1-31.

i-scoop. (2021). *Edge computing – the what, how and where of the edge.* Retrieved from https://www.i-scoop.eu/edge-computing-explained/

i-scoop. (n.d.). *Building management in the age of IP and IoT (interview).* Retrieved from https://www.i-scoop.eu/internet-of-things-iot/building-management-systems-iot/

IDC. (2014). *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination.* Retrieved from http://publications.europa.eu/resource/cellar/35f3eccd-f7ce-11e5-b1f9-01aa75ed71a1.0001.01/DOC_1

IDC. (2019). *The technology impacts of edge computing in europe.* Retrieved from https://www.uk.idc.com/research-uk/RESOURCES/ATTACHMENTS/EUR245277019.pdf

IDC. (2020). *Worldwide Spending on Edge Computing Will Reach $250 Billion in 2024.* Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS46878020

IEEE IoT Technical Community. (2020). Retrieved from IEEE IoT: https://iot.ieee.org/definition.html

IESE. (2018). *New York, London and Paris Firmly Established as the Smartest Cities .* Retrieved from https://www.ieseinsight.com/doc.aspx?id=2124&ar=&idi=2&idioma=2

IHS Markit. (2018). *8 in 2018: The top transformative technologies to watch this year.* Retrieved from IHS Markit: https://cdn.ihs.com/www/pdf/IHS-Markit-2018-Top-Transformative-Technology-Trends.pdf

IndustryARC. (2020). *Edge Computing Market - Forecast(2021 - 2026).* Retrieved from https://www.industryarc.com/Report/17939/edge-computing-market.html

Insight Partners. (2019). *Europe 5G in IoT Market to 2027*. Retrieved from https://www.reportlinker.com/p05828373/Europe-5G-in-IoT-Market-to-Regional-Analysis-and-Forecasts-by-Radio-Technology-Device-Range-End-User-Industry.html?utm_source=GNW

IoF. (2020). *IMPACT.* Retrieved from https://www.iof2020.eu/about/impact

IoT Analytics. (2018). *State of the IoT.* Retrieved from IoT Analytics: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

iot-open.eu. (2016). Retrieved from Project IoT-Open: http://iot-open.eu/

ISO. (2018). *IoT Reference Architecture*. Retrieved from https://www.iso.org/standard/65695.html

ISO. (2020). *ISO/IEC TR 23188: Information technology — Cloud computing — Edge computing landscape.* IOS/IEC.

ITU. (2012). *Overview of the Internet of things*. Retrieved from https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

ITU. (2019). *Architectural reference models of devices for Internet of things applications*. Retrieved from https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.4460

ITU. (2020). *Measuring Digital Development: Facts and Figures*. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf

ITU. (2021). *Episode #12: Interoperability of IoT and satellite data for Earth observation supporting sustainable development.* Retrieved from https://www.itu.int/en/ITU-T/webinars/20210909/Pages/default.aspx

Jamshidi, M. (2008). An integration of a finite number of constituent systems which are independent and operatable, and which are networked together for a period of time to achieve a certain higher goal. In *Systems of Systems Engineering: Principles and Applications.*

Kaloudi, N. &. (2020). The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR), 53(1)*, 1-34.

Kearney. (2015). *Rebooting Europe's high-tech industry.* Retrieved from https://www.de.kearney.com/communications-media-technology/article?/a/rebooting-europes-high-tech-industry

Khan, J. (2021). *European academic brain drain: A meta-synthesis.* Retrieved from Wiley Online Library: https://onlinelibrary.wiley.com/doi/10.1111/ejed.12449?af=R

KPMG. (2018). *The Changing Landscape of Disruptive Technologies*. Retrieved from https://assets.kpmg/content/dam/kpmg/pl/pdf/2018/06/pl-The-Changing-Landscape-of-Disruptive-Technologies-2018.pdf

LFEdge. (2020). *State of the Edge 2020.* Retrieved from https://www.lfedge.org/wp-content/uploads/2020/04/SOTE2020.pdf

LSP - CREATE IoT. (2019). *The European Large-Scale Pilots Programme Driving IoT Innovation at Scale in Europe.* Retrieved from https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf

McKinsey. (2017). *Smartening up with Artificial Intelligence (AI) - What’s in it for Germany and its Industrial Sector?* Retrieved from https://www.mckinsey.com/~/media/McKinsey/Industries/Semiconductors/Our%20Insights/Smartening%20up%20with%20artificial%20intelligence/Smartening-up-with-artificial-intelligence.ashx

McKinsey. (2020). *Europe’s start-up ecosystem: Heating up, but still facing challenges.* Retrieved from https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/europes-start-up-ecosystem-heating-up-but-still-facing-challenges

McKinsey. (2020). *The 5G era.* Retrieved from https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/the%205g%20era%20new%20horizons%20for%20advanced%20electronics%20and%20industrial%20companies/the-5g-era-new-horizons-for-advanced-electronics-and-industrial-compan

McKinsey. (2021). *Europe's digital migration during COVID-19: Getting past the broad trends and averages*. Retrieved from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/europes-digital-migration-during-covid-19-getting-past-the-broad-trends-and-averages

McKinsey&Company. (2018). *New demand, new markets: What edge computing means for hardware companies*. Retrieved from https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/New%20demand%20new%20markets%20What%20edge%20computing%20means%20for%20hardware%20companies/New-demand-new-markets-What-edge-comp

Minerva, R., Abyi, B., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). *IEEE Internet Initiative 1.1*, 1-86.

Mlitz, K. (2021). *ICT industry full-time employment worldwide.* Retrieved from https://www.statista.com/statistics/1126677/it-employment-worldwide/

Mobidev. (2018). *Energy 4.0.* Retrieved from https://mobidev.biz/blog/digital-transformation-energy-utilities-sector

Mordor Intelligence. (2021). *INTERNET OF THINGS (IOT) MARKET - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2021 - 2026)*. Retrieved from https://www.mordorintelligence.com/industry-reports/internet-of-things-moving-towards-a-smarter-tomorrow-market-industry

NGI.eu. (2019). *Next Generation Internet.* Brussels.

NGI.eu. (2020). *Internet of humans.* Retrieved from https://www.ngi.eu/news/2019/09/18/next-generation-internet-the-internet-of-humans/

NGIoT Consortium. (2018). *Description of Action.* Brussels.

NGIoT Consortium. (2020). *D1.1 Ecosystem Building Vision and Report.* Brussels.

NGIoT Consortium. (2021). *IoT Ecosystem Building Vision and Report.* Retrieved from NGIOT.

NGIoT D1.1. (2021). *IoT Ecosystem Building Vision and Report*. Retrieved from NGIoT Deliverables: https://www.ngiot.eu/deliverables/

NGIoT D2.1. (2021). *Next Generation Internet of Things*. Retrieved from https://www.ngiot.eu/deliverables/

Nokia Bell Labs. (2019). *5G for Future Industrial Internet.* Retrieved from https://www.traficom.fi/sites/default/files/media/file/Putkonen%20Jyri_5GMomentum_5GIIoT_JPutkonen_20191029.pdf

Novarica. (2017). *Big Data, IoT, and AI Maturity Levels.* Retrieved from https://aite-novarica.com/report/big-data-iot-and-ai-maturity-levels

NSB. (2018). *Publications Output: U.S. Trends and International Comparisons* . Retrieved from https://ncses.nsf.gov/pubs/nsb20206/

OECD. (2018). *Promoting innovation in established SMEs*. Retrieved from https://www.oecd.org/cfe/smes/ministerial/documents/2018-SME-Ministerial-Conference-Parallel-Session-4.pdf

Open Access Government. (2020). *The cybersecurity challenges of 5G and IoT*. Retrieved from https://www.openaccessgovernment.org/the-cybersecurity-challenges-of-5g-and-iot/85940/

Osborne Clark. (2015). *Smart Cities in Europe.* Retrieved from https://www.osborneclarke.com/media/filer_public/b3/bc/b3bcaffa-2b02-465d-804d-af85d735e8e9/smart_cities_in_europe_e-version.pdf

OVHCloud. (2021). *The European Cloud industry.* Retrieved from https://corporate.ovhcloud.com/en/newsroom/news/europe-cloud-challenges-key-and-five-scenarios-impact/

Pannier, A. (2021). *Europe in the Geopolitics of Technology Connecting the Internal and External Dimensions.* Retrieved from https://www.ifri.org/sites/default/files/atoms/files/pannier_europe_geopolitics_technology_2021_.pdf

PwC. (2016). *The Internet of Things: Is it just about GDPR?* Retrieved from https://www.pwc.co.uk/services/risk/technology-data-analytics/data-protection/insights/the-internet-of-things-is-it-just-about-gdpr.html

Roland Berger. (2014). *INDUSTRY 4.0 The new industrial revolution How Europe will succeed.* Retrieved from https://www.iberglobal.com/files/Roland_Berger_Industry.pdf

Roland Berger. (2018). *Artificial Intelligence – A strategy for European startups*. Retrieved from https://www.rolandberger.com/publications/publication_pdf/roland_berger_ai_strategy_for_european_startups.pdf

Sahin, K., & Barker, T. (2021). *Europe's Capacity to Act in the Global Tech Race Charting a Path for Europe in Times of Major Technological Disruption.* Retrieved from https://dgap.org/sites/default/files/article_pdfs/210422_report-2021-6-en-tech.pdf

Santarsiere, R. (2019). *Prolonged geopolitical and economic uncertainty see foreign direct investment into Europe drop for the first time in six years.* Retrieved from https://www.ey.com/en_gl/news/2019/06/prolonged-geopolitical-and-economic-uncertainty-see-foreign-direct-investment-into-europe-drop-for-the-first-time-in-six-years

SAP. (2021). *Use Cases*. Retrieved from https://www.sap.com/products/business-technology-platform/use-cases.html?sort=title_asc

Schirmeier, Q. (2021). How Europe's €100-billion science fund will shape 7 years of research. *Nature*, 20-21.

Schlaak, T., & Truby, J. (2021, July). *The future of power.* Retrieved from Deloitte: https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/renewable-power-generation-in-europe.html

Schladofsky, W., Mitic, J., Megner, A., Simonato, C., Gioppo, L., Leonardos, D., & Bröring, A. (2017). *Business Models for Interoperable IoT Ecosystems.* Retrieved from https://www.researchgate.net/publication/315786719_Business_Models_for_Interoperable_IoT_Ecosystems

Seliem, M. E. (2018). Towards privacy preserving iot environments: a survey. *Wireless Communications and Mobile Computing*.

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

SRIA. (2017). *Language Technologies for Multilingual Europe.* Retrieved from http://www.cracking-the-language-barrier.eu/wp-content/uploads/SRIA-V1.0-final.pdf

Synchronicity. (2019). *Reference Architecture for IoT Enabled Smart Cities*. Retrieved from https://synchronicity-iot.eu/wp-content/uploads/2018/09/SynchroniCity_D2.10.pdf

Taylor, C. (2018). *Europe aims to have 300 smart cities by end of next year.* Retrieved from https://energypost.eu/europe-aims-to-have-300-smart-cities-next-year/

Thales Group. (2021). *BEYOND GDPR: DATA PROTECTION AROUND THE WORLD.* Retrieved from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/magazine/beyond-gdpr-data-protection-around-world

Warnat-Herresthal, S. e. (2021). Swarm Learning for decentralized and confidential clinical machine learning. *Nature 594.7862*, 265-270.

WBC-RTI. (2016). *ICT RESEARCH & INNOVATION*. Retrieved from https://wbc-rti.info/theme/34

Willner, A. &. (2020). Towards a Reference Architecture Model for Industrial Edge Computing. *IEEE Communications Standards Magazine 4.4*, 42-48.

Zhu, Q. L.-R. (2019). Applications of distributed ledger technologies to the internet of things: A survey. *ACM computing surveys (CSUR), 52(6)*, 1-34.

ZVEI. (2018). Reference Architectural Model Industrie 4.0 (RAMI4.0) - An Introduction. *Plattform Industrie 4.0*.