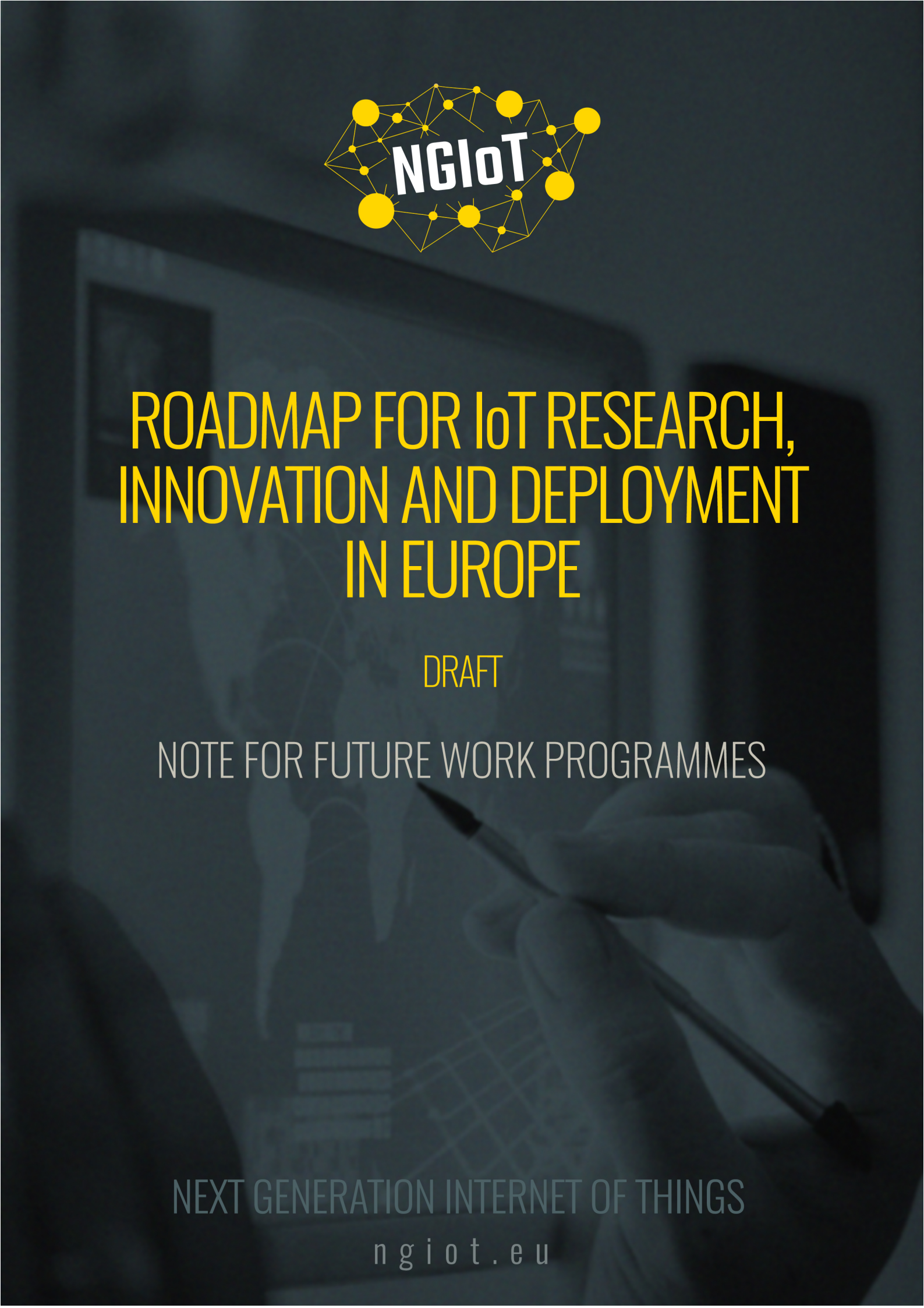


ROADMAP FOR IoT RESEARCH, INNOVATION AND DEPLOYMENT IN EUROPE

DRAFT

NOTE FOR FUTURE WORK PROGRAMMES

NEXT GENERATION INTERNET OF THINGS

ngiot.eu

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

Next Generation Internet of Things

Lead Editors	Martin Brynskov (Aarhus University), Federico Michele Facca (Martel Innovate), Pasquale Annicchino (Archimede Solutions)
Contributors (in alphabetical order)	Martin Brynskov (Aarhus University), Monique Calisti (Martel Innovate), Benoît Dalbert (Aarhus University), Federico Michele Facca (Martel Innovate), Adriënne Heijnen (Aarhus University), Pasquale Annicchino (Archimede Solutions), Lamprini Kolovou (Martel Innovate).
Version	1.0
Date	31st January 2020

Feedbacks

NGIoT consortium welcomes feedbacks! Use the QR Code (or the following link: https://forms.gle/JVaXya1nwMLb3tGr7) on the side to access a feedback form.
The feedbacks will be used for the roadmap activities of NGIoT.

Important Notice: Working Document

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

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

TABLE OF CONTENT

1. INTRODUCTION

This draft roadmap for IoT research, innovation and deployment in Europe aims to provide a concise and actionable view of the European Union (EU) priorities for the 2021-2027 programming period in relation to the Internet of Things (IoT) technologies and their challenges not only in the Research and Innovation agenda but also in the Deployment agenda that fosters the take-up of mature IoT solutions.

The work presented in this note draws on the findings of the Scoping Paper "Building a Roadmap for the Next Generation Internet of Things: Research, Innovation and Implementation"[1] which was released in September 2019 by the NGIoT Coordination and Support Action (CSA) funded by the Horizon 2020 programme. It should be regarded as an intermediary step towards the final IoT roadmap for Europe, which is scheduled for 2021.

In particular, this draft roadmap complements the Scoping Paper as follows:

i) It provides an updated view of the EU Strategy and Policy context while taking into consideration the latest communications and policy developments;

ii) It introduces novel and revised challenges connected to the debate occurred within the NGIoT Strategy Board;

iii) It projects on a timeline the topics related to those challenges;

iv) It makes a series of structured recommendations for the upcoming work programmes.

2. EU STRATEGY AND POLICY CONTEXT

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

- A Europe fit for the digital age[2], by empowering people with a new generation of technologies and sustaining the Digital Single Market[3] Strategy to create better and larger opportunities for European companies, not only in cities but also in rural and periurban areas;
- A new agenda for the European strategic autonomy[4] that encompasses the changes brought

[1] https://ngiot.eu/wp-content/uploads/sites/26/2019/09/NGIoT_scoping-paper.pdf

[2] https://ec.europa.eu/info/priorities/europe-fit-digital-age_en

[3] EC. A Digital Single Market Strategy for Europe. 2015

[4] EC. Rethinking Strategic Autonomy in the Digital Age. 2019

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 application of the EU Charter of Fundamental Rights through laws and policies, including Data Protection[5];
- A new European Green Deal[6], a set of policies to ensure the sustainability of the EU economy.

Within the Digital Single Market Strategy, the Internet of Things (IoT) represents the next step of disruptive digital innovation where 'any physical and virtual object can be connected to other objects and to the Internet, creating a fabric of connectivity between things and between humans and things.' The Internet of Things, in combination with cloud and edge computing, Artificial Intelligence, and 5G will contribute to profoundly transforming the EU economy and society.

"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 – in urban, periurban and rural areas.

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

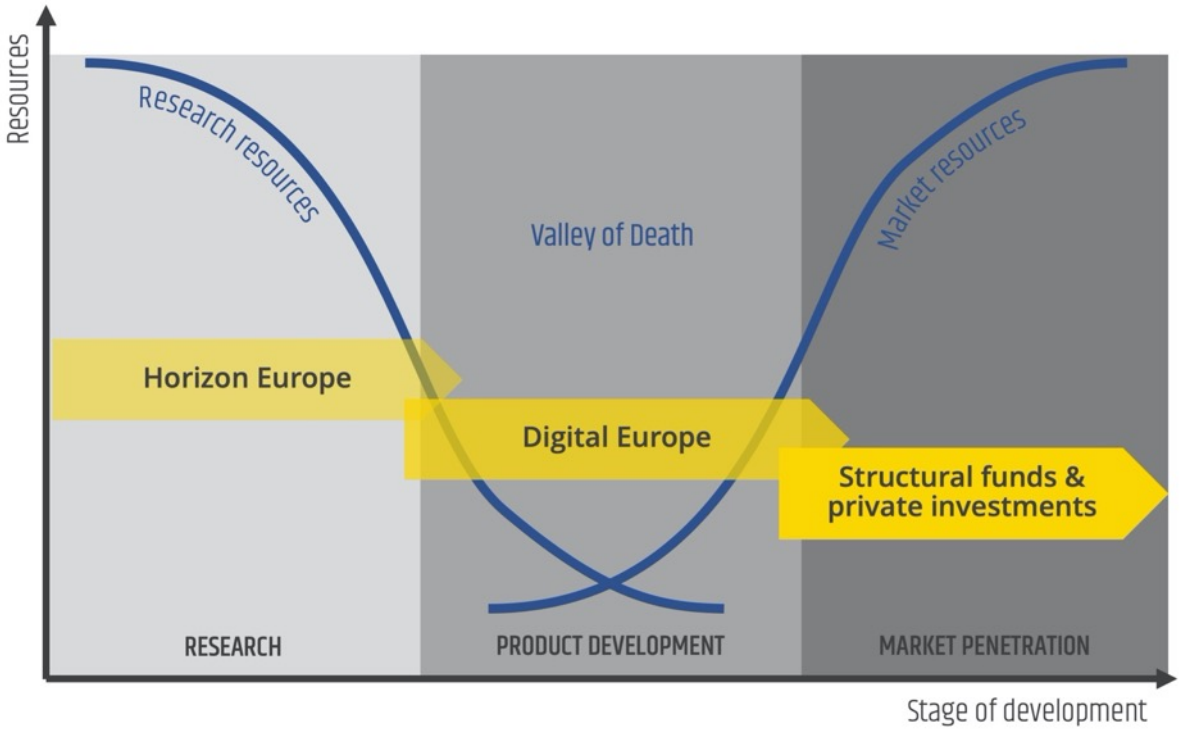
- Horizon Europe, the new research and innovation programme to succeed Horizon 2020 with a proposed € 100 billion budget, including € 15 billion on the 'Digital, Industry and Space' cluster.
- Digital Europe, a brand new programme focusing on building the strategic digital capacities of the EU and on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

These three programmes are meant to complement each other and will play a key role in Europe's digitalisation in connection with the Internet of Things technologies. While Horizon Europe will provide future outlook by supporting cutting edge research and innovation, Digital Europe and Connecting Europe Facility will foster the market deployment of mature technologies (including those that proved maturity and business viability from Horizon 2020 and, in future, Horizon Europe). The introduction of the Digital Europe programme may play a key role in supporting the deployment

[5] EC. General Data Protection Regulation (EU) 2016/679 (GDPR). 2016

[6] EC. Communication on The European Green Deal. 2019

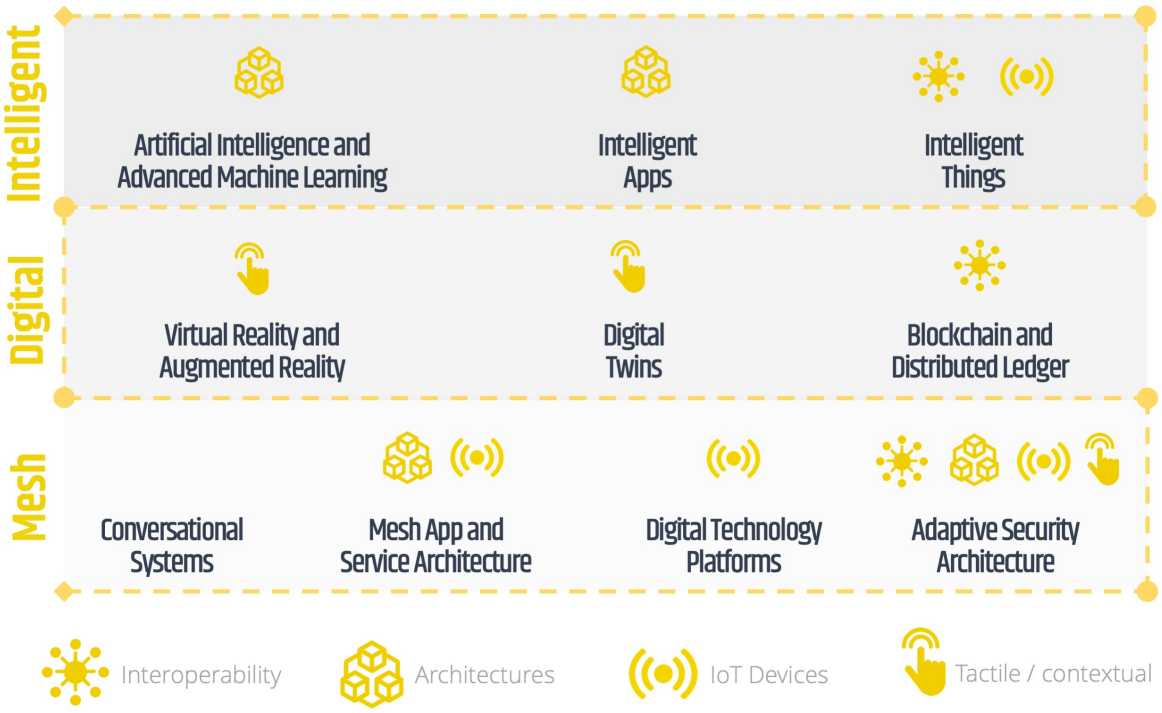
of mature research and innovation outcomes, bridging them between the Research and Market penetration phases, thus helping to overcome the so-called “Valley of Death”.



3. TECHNOLOGY CONTEXT

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, also from a territorial perspective.

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. The human-centred Internet has become central to the EU vision for digital technologies under the umbrella of the Next Generation Internet (NGI) initiative starting from the Horizon 2020 ICT Work Programme 2016-2017 and reinforced in its version for 2018-2020.



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

- **Edge Computing**, enabling local decisions in a reliable way (i.e. regardless of connectivity with the cloud) to IoT solutions.
- **5G**, providing cheap, reliable and scalable internet connectivity to IoT networks.
- **Artificial Intelligence and analytics**, enabling extraction of unexpected 'intelligence' from sensed data, the automatic actuation based on 'intelligent' models (e.g. self-driving cars), and the higher automation in the management of a plethora of devices and their generated data.
- **Augmented Reality and Tactile Internet**, creating interactive, conversational IoT platforms with new user interfaces to engage with things and humans, adding the human-centred perspective and sensing/actuating capabilities to the human-objects-systems interaction.
- **Digital Twin**, realising the digital replica of a living or non-living physical entity and exploring the 'human' side of the interaction between humans and machines.
- **Distributed Ledgers**, enabling decentralised data governance and thus ensuring truthfulness of the data.

4. SUMMARY OF KEY R&I&D CHALLENGES

- **Reliable, low-cost, sustainable and scalable IoT networks (R1)**. 5G and its evolution should go further to address the low cost, massive IoT device deployment. Such technologies also need to be sustainable by limiting the usage of resources and their impact on the

environment, to avoid the large-scale deployment of devices becoming unsustainable from an environmental point of view.

- **Next Generation IoT data processing architectures (R2)**. Real-time analytics architectures need to evolve, ensuring the capacity required by massive IoT deployments. Processing functions - to increase their speed - will need to be directly available at the level of processing units.

- **Futureproof security and trust (R3).** Research should focus on 'intelligent' approaches to security, i.e. on the ability to 'learn' new attack patterns and derive counter solutions autonomously. Solutions linked to ensuring trust and traceability of IoT data should scale, coping with requirements posed by real-time data scenarios in several IoT market segments.

- **IoT, processes, and data interoperability (R4)**. Data interoperability remains a key challenge in the IoT arena. Research should explore a pragmatic approach, where semi-automatic interoperability is achieved through limited human interaction. With the increasing platform-to-platform communication, it will also require solutions for IoT-driven processes interoperability. Novel scalable and reliable solutions are required to this end.

- **IoT, citizens, privacy-by-design, and ethics (R5)**. To understand and forecast the impact of IoT solutions on society, Europe needs a multidisciplinary approach embracing legal, sociological and ethical research in relation to the adoption of IoT and connected technologies, such as Artificial Intelligence.

- **Real-time decision making for IoT (R6)**. Future IoT solutions should be able to coordinate real-time decision making based on a widely distributed and decentralised infrastructure, so as to achieve a common goal. Decision-making will also need to take into account the 'human' factor, and the underlying ethical aspects.

- **Autonomous IoT solutions (R7)**. To enable large scale IoT deployments, future solutions should be largely autonomous and able to transform C-level KPIs into corresponding actions at the different layers of the IoT stack.

- **Human and sustainable development in the loop IoT (R8)**. Future IoT solutions should support interaction with humans and enable them to make informed decisions. To better fulfil future human needs, IoT solutions should also become sustainable by design, not only supporting the development of solutions improving sustainability, but also becoming sustainable themselves.

- **IoT data sharing and monetisation enabling models and technologies (R9)**. Research and innovation should find novel solutions to increase the trust toward data sharing and the feeling of data control by owners. New models to incentivise data sharing are key.

- **Sustainable and biocompatible devices (R10)**. Recent advancements in biotechnologies and nanotechnologies should be exploited to experiment the development of IoT devices that dramatically reduce energy consumption (increasing their lifespan) and the development of sensors that are biocompatible (and hence to do not pollute environment) and aim at biodegradability.

5. CHALLENGES, TOPICS AND TIMELINE

The above challenges that are discussed in more detail in the Scoping Paper correspond to the different topics that are key for the evolution of IoT research in the next few years. To facilitate the analysis of priorities for the upcoming work programmes, we have:

i) Grouped such topics within the challenges and mapped them on a timeline corresponding to upcoming work programmes' timelines[7], i.e. 2021-2022, 2023-2024 and 2025-2027;

ii) Mapped them to research (R), innovation (I) and deployment (D) based on the current or forecasted maturity[8];

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

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

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

The table below summarises the exercise we conducted, while in the next paragraphs we provide a short discussion for the time frames covered. Obviously, taking into consideration the rapid evolution of digital technologies, the medium-term (2023-2024) and longer term (2025-2027) timelines will require additional updates and reassessments in the future.

[7] The mapping to timeline and maturity forecast are based on insights from IoT Analytics, "2019 IoT Emerging Technology Radar", 2019 and Gartner, "Hype Cycle for the Internet of Things, 2019"

[8] See footnote 7.

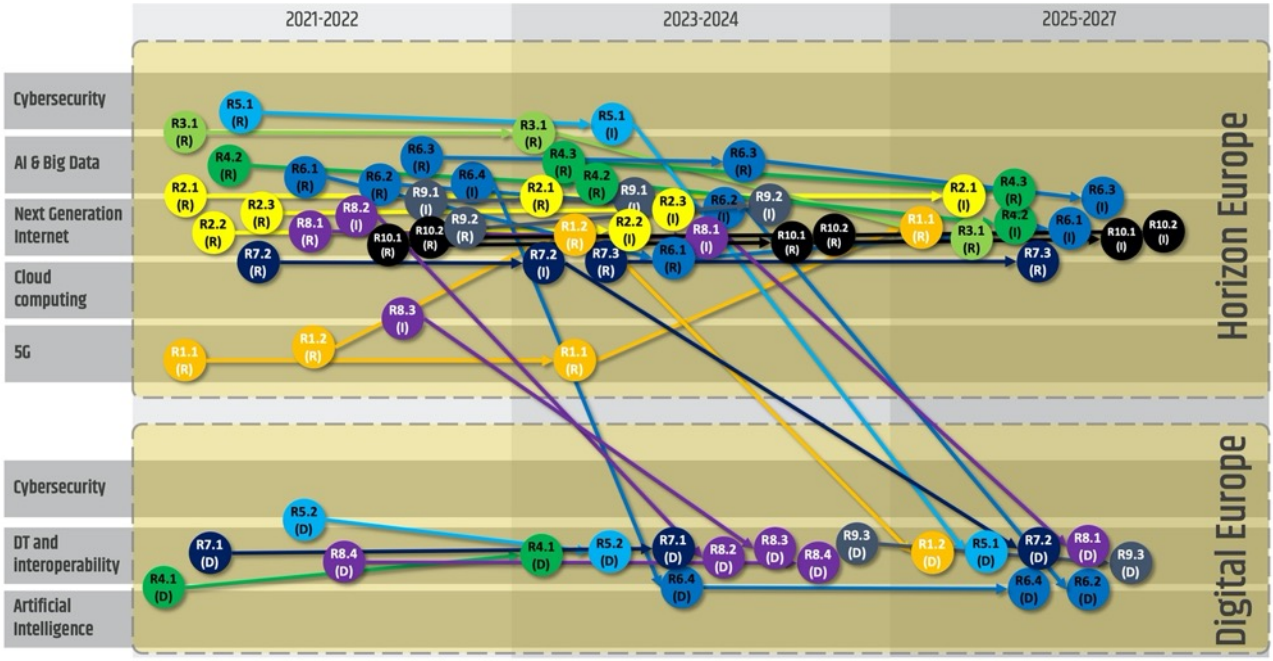
	Timeline		
Challenge	**2021-2022**	**2023-2024**	**2025-2027**
Reliable, low-cost, sustainable and scalable IoT networks (R1)	R1.1 - Low-cost, high-volume connectivity (R) [5G] R1.2 - Low-power connectivity schemes (R) [5G]	R1.1 - Low-cost, high-volume connectivity (R) [5G] R1.2 - Low-power connectivity schemes (I) [5G/IoT]	R1.1 - Low-cost, high-volume connectivity (I) [5G/IoT] R1.2 - Low-power connectivity schemes (D) [IoT]
Next Generation IoT data processing architectures (R2)	R2.1 Novel data processing architectures (R) [IoT/DM] R2.2 IoT data processing optimised micro CPUs (R) [IoT/CPS] R2.3 Highly scalable and low latency ledgers for IoT (R) [IoT/DL]	R2.1 Novel data processing architectures (R) [IoT/DM] R2.2 IoT data processing optimised micro CPUs (I) [IoT/CPS] R2.3 Highly scalable and low latency ledgers for IoT (I) [IoT/DL]	R2.1 Novel data processing architectures (I) [IoT/DM] R2.2 IoT data processing optimised micro CPUs (D) [IoT/CPS] R2.3 Highly scalable and low latency ledgers for IoT (D) [IoT/DL]
Futureproof security and trust (R3)	R3.1 Novel future proof cybersecurity (R) [CS/AI] R3.2 IoT data traceability and trust (I) [IoT/DL]	R3.1 Novel future proof cybersecurity (R) [CS/AI] R3.2 IoT data traceability and trust (D) [IoT/DL]	R3.1 Novel future proof security mechanisms for IoT (R) [IoT]
IoT, processes, and data Interoperability (R4)	R4.1 IoT data dictionaries deployed at scale (D) [IoT] R4.2 Semi-automated data interoperability (R) [AI/DM]	R4.1 IoT data dictionaries deployed at scale (D) [IoT] R4.2 Semi-automated data interoperability (R) [AI/DM/IoT] R4.3 Semi-automated process interoperability (R) [AI/DM]	R4.2 Semi-automated data interoperability (I) [AI/DM/IoT] R4.3 Semi-automated process interoperability (R) [AI/DM/IoT]

	Timeline		
Challenge	**2021-2022**	**2023-2024**	**2025-2027**
IoT, citizens, privacy-by-design, and ethics (R5)	R5.1 Privacy-by-design for IoT devices (R) [IoT/CPS/CS] R5.2 Security & Privacy-by-design for IoT services (D) [IoT/CPS/CS]	R5.1Privacy-by-design for IoT devices (I) [IoT/CPS/CS] R5.2 Security & Privacy-by-design for IoT services (D) [IoT/CPS/CS]	R5.1Privacy-by-design for IoT devices (D) [IoT/CPS/CS]
Real time decision-making for IoT (R6)	R6.1 Dynamic orchestration of decentralised AI pipelines (R) [CC/AI] R6.2 Native AI-capable devices (R) [CPS/AI] R6.3 AI for Humans: understandable and ethical decisions (R) [AI] R6.4 Validated AI algorithms for IoT use cases (I) [AI/IoT]	R6.1 Dynamic orchestration of decentralised AI pipelines (R) [CC/AI/IoT] R6.2 Native AI-capable devices (I) [CPS/AI/IoT] R6.3 AI for Humans: understandable and ethical decisions (R) [AI] R6.4 Validated AI algorithms for IoT use cases (D) [AI/IoT]	R6.1 Dynamic orchestration of decentralised AI pipelines (I) [CC/AI/IoT] R6.2 Native AI-capable devices (D) [CPS/AI/IoT] R6.3 AI for Humans: understandable and ethical decisions (I) [AI/IoT] R6.4 Validated AI algorithms for IoT use cases (D) [AI/IoT]
Autonomous IoT solutions (R7)	R7.1 Large IoT & digital infrastructures (D) [IoT] R7.2 Semi-autonomous IoT infrastructures (R) [IoT/CC]	R7.1 Large IoT & digital infrastructure (D) [IoT] R7.2 Semi-autonomous IoT infrastructures (I) [IoT/CC] R7.3 Autonomous IoT infrastructures (R) [IoT/CC]	R7.2 Semi-autonomous IoT infrastructures (D) [IoT/CC] R7.3 Autonomous IoT infrastructures (R) [IoT/CC]
Human and sustainable development in the loop IoT (R8)	R8.1 Sustainable IoT by design (R) [IoT] R8.2 Augmented IoT (I) [HCI/IoT] R8.3 Tactile Internet	R8.1 Sustainable IoT by design (I) [IoT] R8.2 Augmented IoT (D) [HCI/IoT] R8.3 Tactile Internet	R8.1 Sustainable IoT by design (D) [IoT] R8.4 IoT for sustainability (D) [IoT]

	Timeline		
Challenge	**2021-2022**	**2023-2024**	**2025-2027**
	(I) [5G/HCI/IoT] R8.4 IoT for sustainability (D) [IoT]	(D) [5G/HCI/IoT] R8.4 IoT for sustainability (D) [IoT]	
IoT data sharing and monetisation enabling models and technologies (R9)	R9.1 IoT data market architectures (I) [DL/DM/IoT] R9.2 Novel business models to incentivise data sharing (R) [IoT/DM]	R9.1 IoT data market architectures (I) [DL/DM/IoT] R9.2 Novel business models to incentivise data sharing (I) [IoT/DM] R9.3 Large data marketplaces for IoT scenarios (D) [DL/DM/IoT]	R9.3 Large data marketplaces for IoT scenarios (D) [DL/DM/IoT]
Sustainable and biocompatible devices (R10)	R10.1 Energy (semi)-autonomous devices (R) [IoT/CPS] R10.2 Bio-compatible sensors (R) [IoT/CPS]	R10.1 Energy (semi)-autonomous devices (R) [IoT/CPS] R10.2 Bio-compatible sensors (R) [IoT/CPS]	R10.1 Energy (semi)-autonomous devices (I) [IoT/CPS] R10.2 Bio-compatible sensors (I) [IoT/CPS]
Large Scale Pilots	V1. Agriculture (D) V2. Smart Cities (D) V3. Healthcare (D) V4. Manufacturing (D) V5. Energy Management (I) V6. Insurance (I) V7. Media (R) V8. Transportation (R) V9. Safety & Defence (R)	V1. Agriculture (D) V2. Smart Cities (D) V3. Healthcare (D) V4. Manufacturing (D) V5. Energy Management (D) V6. Insurance (D) V7. Media (I) V8. Transportation (I) V9. Safety & Defence (I)	V7. Media (D) V8. Transportation (I) V9. Safety & Defence (D)

6. RECOMMENDATIONS FOR FUTURE WORK PROGRAMMES

In this section, we provide a time frame for a set of recommendations for Horizon Europe and Digital Europe based on the analysis conducted and summarised in the previous section. The following figure presents the outcomes of the analysis, mapping them to the key ICT areas covered in Horizon Europe and Digital Europe. As successful digital transformation is key for Europe's future, the territorial approach should also be considered, when relevant.



6.1. Key recommendations for 2021-2022

Recommendations for the Horizon Europe programme

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

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

- Focus on the **transition from data management to insight generation from data** by delivering ready-to-use AI algorithms in different scenarios (R6.4 - IA) and on the increase of

automation **to reduce the cost of the management of complex IoT platforms** and networks focusing on semi-automatic approaches as a first step (R7.2 - RIA / R4.2 - RIA).

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

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

- **Support the establishment of large IoT trials in new domains** beyond the ones covered today by the IoT Large Scale Pilots[9] (LSPs), such as Energy Management, Insurance (IA) and Media, Transportation, and Safety & Defence (RIA).

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

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

Recommendations for the Digital Europe programme

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

- **Facilitate access to large computational facilities needed to harness the complexity of analysing terabytes** (or petabytes) of IoT generated data and ensure sovereignty by deploying large scale (federated) digital infrastructures across Europe (R7.1).

- Sustain the **development and uptake of cross-domain harmonised data models**, following the path established by OASC[10], to **increase IoT application interoperability and replicability** especially in the public sector across Europe (R4.1), fostering them as requirements in related public procurements.

- **Transfer the experience matured by running LSPs** in the sectors of Smart Cities, Agriculture and Healthcare to a wider set of actors **through Innovation Procurement** and similar actions.

- **Deploy secure and highly scalable IoT and digital infrastructures** (R7.1) with special focus on edge capacity, leveraging on global networking technologies such as IPv6 and 5G.

---

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

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

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

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

6.2. Key recommendations for 2023-2024

Recommendations for the Horizon Europe programme

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

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

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

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

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

- **Support the establishment of large IoT trials in new domains** beyond the ones covered today by IoT LSPs, such as Media, Transportation, and Safety & Defence (IA).

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

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

Recommendations for the Digital Europe programme

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

- **Facilitate access to large computational facilities needed to harness the complexity of analysing terabytes** (or petabytes) of IoT generated data and ensure sovereignty by deploying large scale (federated) digital infrastructures across Europe (R7.1).

- Sustain the **development and uptake of cross-domain harmonised data models**, following the path established by OASC, to **increase IoT application interoperability and replicability** especially in the public sector across Europe (R4.1).

- **Transfer the experience matured by running LSPs** in the sectors of Smart Cities, Agriculture, Healthcare, Manufacturing, Energy Management and Insurance to a wider set of actors **through Innovation Procurement** and similar actions.

- **Deploy secure and highly scalable IoT and digital infrastructures** (R7.1, R8.2, R8.3, R9.3) with special focus on edge capacity and ability to create large IoT markets for augmented and tactile internet, leveraging on global networking technologies such as IPv6 and 5G.

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

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

6.3. Key recommendations for 2025-2027

Recommendations for the Horizon Europe programme

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

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

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

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

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

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

Recommendations for the Digital Europe programme

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

- **Transfer the experience matured by running LSPs** in the sectors of Media, Transportation, Safety & Defence to a wider set of actors **through Innovation Procurement** and similar actions.

- **Support the creation of a set of open and royalty-free-to-use trustable classification and prediction algorithms covering key sectors of the European economy (R6.4)**.

- **Deploy sustainable and highly scalable IoT and digital infrastructures** (R8.1, R9.3) with special focus on creation of large scale data markets.

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

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

6.4. General Recommendation of cohesive approaches

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

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

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

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

- Support solutions to ***drastically reduce costs of deployment and management of large digital infrastructures***, spanning from the devices at the edge through the network (R1.1) up to data centres (R7.2 / R7.3).

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

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

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

NEXT GENERATION INTERNET OF THINGS

WWW.NGIOT.EU

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