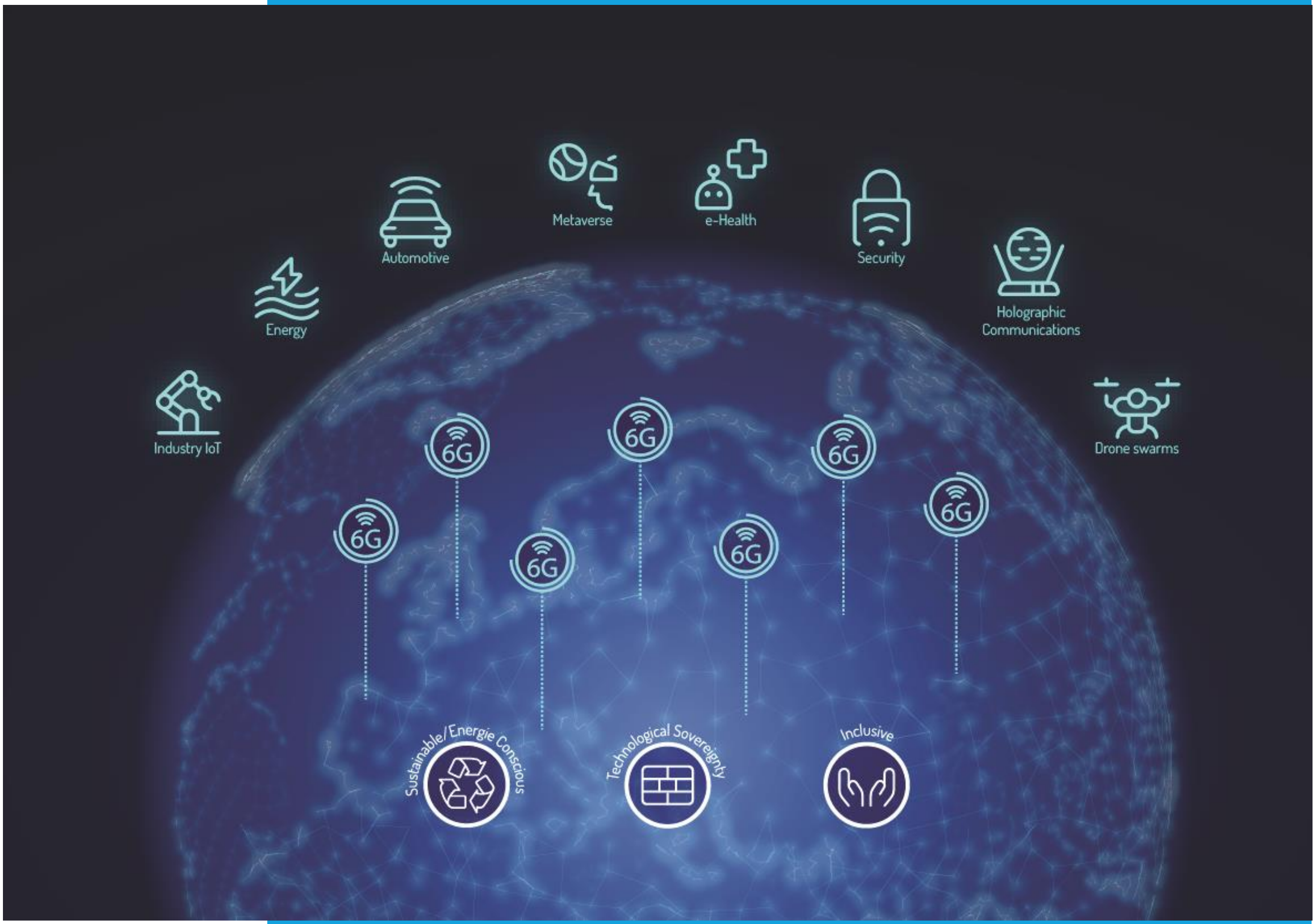
6G Smart Networks and Services Industry Association (6G-IA)



Version 1.0

September 2023

Position paper

KEY STRATEGIES FOR 6G SMART NETWORKS AND SERVICES

DOI: 10.5281/zenodo.8315347
URL: https://6g-ia.eu/plans-papers/

EXECUTIVE SUMMARY

The purpose of this document is to provide a first comprehensive set of key strategic reflections and recommendations for 6G smart networks and services, capturing the views and priorities from the members of the 6G-IA. The goal is that this document will be used to further elaborate future versions of the SNS JU Strategic Research and Innovation Agenda (SRIA) as well as the R&I Work Programmes. It also aims to offer directions for collaboration opportunities for European Stakeholders that will go beyond the scope of the SNS JU. It is the plan of 6G-IA to use this as a "living document" where topics will be updated or highlighted (by producing specific strategic documents) in the coming years, following the technological advances, market uptake and ecosystem evolution.

In this document the following areas are considered and analysed.

- **6G Technological Sovereignty** which includes a) components and microelectronics, b) open SNS solutions, c) cloudification and distributed computing, d) network intelligence, e) security and privacy and f) knowledge base
- **Sustainability** which captures all aspects of environmental, societal and economic sustainability

This document provides a brief analysis of each area and proposes concrete recommendations. The key observations and recommendations of the document are summarized as follows:

<u>Technological sovereignty on components and microelectronics</u>: the target should be to find solutions through research activities that will ensure that supply chains for products, components, materials and know-how are diversified. In terms of European research, the way to address this is through the identification of synergies with related EU Partnerships, so that coherence among research efforts is achieved.

<u>Technological sovereignty on open SNS solutions</u>: Further strengthening of research and innovation activities are needed, ensuring that the results from current activities are capitalized, to reach sound and widely accepted conclusions. All research efforts should work under the assumption of technology-neutral regulation, not mandating any architectures but rather pursuing the most suitable and efficient solutions for the European stakeholders.

<u>Technological sovereignty on cloudification and distributed computing:</u> Further research efforts are needed to ensure Interoperability between cloud infrastructures. That way it is possible to have different independent cloud infrastructures that are separately optimised for a specific task or market. Additionally it is important to identify open-source activities that will support such interoperability. Therefore, it is key to ensure that, where relevant, the produced solutions are integrated with the research and innovation actions being developed in the context of the SNS JU.

Technological sovereignty on network intelligence: Existing results from the 5G PPP era have indicated the need for a globally accepted framework where AI/ML will be benchmarked and validated. Additionally, appropriate training data sets are needed to support such a framework. These can be developed in the context of the research and innovation actions in the context of the SNS JU. To allow interconnection and interoperation of AI, digital twins and other intelligent components across different stakeholders, open solutions and well selected standardised interfaces are needed for training and execution of AI models.

Technological sovereignty on security and privacy: It is important to create a collaborative environment for key public and private forces to cover the complete range of needs from research activities, develop security solutions in critical hardware and software modules and foster solutions that will conform to European policies and legislation by meeting European values.

Technological sovereignty on knowledge experts base: Research and innovation activities should actively contribute towards a timely integration of the knowledge produced by SNS R&I activities in the educational process at the European level and measures to grow the base of experts in Europe.

Sustainability: This is globally accepted as a key target for 6G. Sustainability as a term encompasses both new solutions for sustainable Information and Communication technology (ICT) as well as ICT innovations to support sustainability on all vertical sectors. Therefore, it is imperative to develop a framework that will serve for the quantitative evaluation of solutions designed to support environmental, societal and economical sustainability measured by key value indicators.

In follow-up work and position development the implications of the above will be addressed in the context of and for the anticipation of future developments of the service provider ecosystems and multi-stakeholder service platforms.

TABLE OF CONTENTS

1. INTRODUCTION

The purpose of this document is to provide a first comprehensive set of key strategic reflections and recommendations for 6G smart networks and services, capturing the views and priorities from the members of the 6G-IA. The goal is that this document will be used to further elaborate future versions of the SNS JU Strategic Research and Innovation Agenda (SRIA) as well as the R&I Work Programmes. It also aims to offer directions for collaboration opportunities for European Stakeholders that will go beyond the scope of the SNS JU. It is the plan of 6G-IA to use this as a "living document" where topics will be updated or highlighted (by producing specific strategic documents) in the coming years, following the technological advances, market uptake and ecosystem evolution.

The way we live, work and interact has changed considerably during the past years. The importance of information, how it is exchanged, stored and processed, plays a key factor in all aspects of our civilization. The role of the communication infrastructure and services has now a dominant position for all. It is an undeniable fact that telecommunication technologies and services can improve our lives but is also a double-edged sword that could create significant problems and threats if not addressed properly.

Nowadays, we are witnessing the changes that advancements in 5G networks as well related enablers, like Artificial Intelligence and Machine Learning (AI/ML), High Performance Computing (HPC), Cybersecurity, Internet of Things (IoT), etc., bring for all. Moreover, the technological evolution and its applications keep on progressing at a substantial rate.

The work for 6G Networks and Services has started and multiple activities are taking place at a global level. In Europe, the 6G Smart Networks and Services Industry Association (6G-IA), in collaboration with the supporting Associations NetworldEurope, Alliance for Internet of Things Innovation (AIOTI), CISPE.cloud and NESSI, prepared a proposal for a European Partnership for Smart Networks and Services to be implemented in the context of Horizon Europe Framework (HEU) [1].

In November 2021, the Council Regulation 2021/2085 [2] established the SNS Joint undertaking (JU) [3] as a legal and funding entity as part of the 10 European Partnerships [4] to step up the green and digital transition. The SNS JU enables the pooling of EU's industrial and academic/research resources in Smart Networks and Services. It also fosters alignment with EU Member States for 6G Research and Innovation, and deployment of advanced 5G networks. The SNS JU sets out an ambitious mission with an EU funding budget of € 900 million for the period 2021-2027.

As indicated in the official website, the Smart Networks and Services (SNS) Joint Undertaking (JU) has two main missions:

1. **Fostering Europe's technology and digital service sovereignty in 6G** by implementing the related research and innovation (R&I) programme leading to the conception and standardisation starting around 2025. It encourages preparation for early market adoption of 6G technologies and digital services by the end of the decade. Mobilising a broad set of stakeholders is key to address strategic areas of the network technologies and services value chain. This ranges from network edge-

and cloud-based service provisioning to market opportunities in new components and devices beyond smartphones.
2. **Boosting 5G deployment in Europe** in view of developing digital lead markets and enabling the digital and green transition of the economy and society. To address this objective, the SNS JU coordinates strategic guidance for the relevant programmes under the Connecting Europe Facility [5], in particular 5G Corridors. It also contributes to the coordination of national programmes, including the Recovery and Resilience Facility [6] and other European programmes and facilities such as the Digital Europe Programme (DEP) [7] and InvestEU.

The SNS JU also supports technological sovereignty for Europe, in line with the 5G Cybersecurity Toolbox [8], the Cybersecurity Strategy [9] and the industrial strategy [10].

The partnership enables a solid research and innovation (R&I) roadmap [11] as well as a deployment agenda [12] set out and followed by a critical mass of European actors. Already, this roadmap is being implemented through the first SNS R&I Work Programmes [13].

As scientific and technological breakthroughs keep on evolving, it is of paramount importance for **the European industry, the Research Community and Academia** not only to follow these developments, but also to **have a clear strategy** on how Europe should position itself to:

a. Ensure European leadership for 6G smart networks and services through the development of advanced systems, applications and services, design and offer competitive connectivity solutions considering the full value chain, and contribute to technological sovereignty,
b. Improve the digital industries operation by identifying needs and offer solutions, provide advanced infrastructures, and create a fertile business ecosystem,
c. Address societal needs and policy objectives by meeting relevant Sustainable Development Goals (UN SDGs [14]), support the EU Green Deal targets, and safeguard security and privacy.

In this document the following areas are considered and analysed in the following subsections. These strategies are divided in two main pillars as shown in Figure 1.

- **6G Technological Sovereignty** which includes a) components and microelectronics, b) Open SNS solutions, c) cloudification and distributed computing, d) network intelligence, e) security and privacy and f) knowledge base
- **Sustainability** which captures all aspects of environmental, societal and economic sustainability

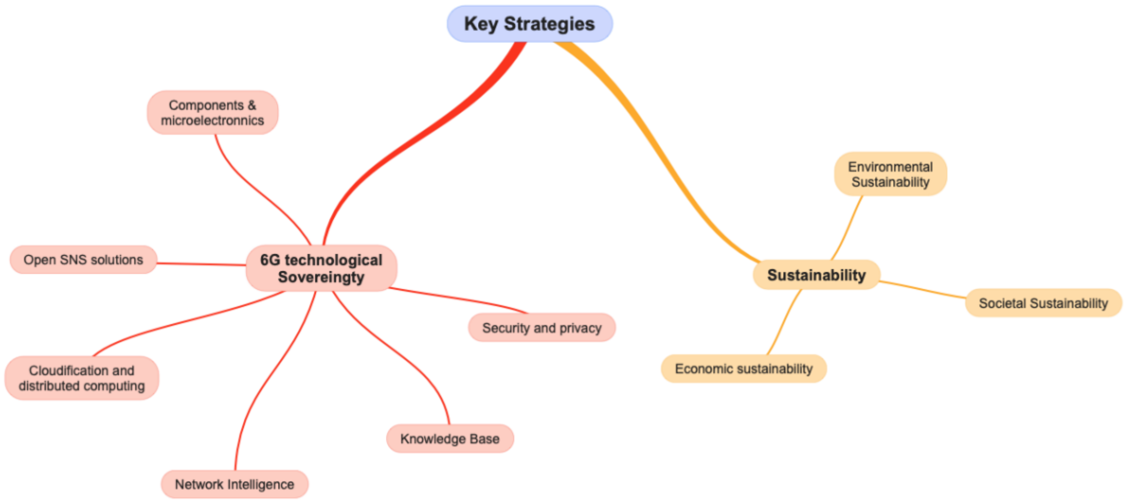


Figure 1: 6G-IA first set of key strategic areas for 6G smart networks and services

Finally, it is very important that all key stakeholders from the private, public, research and educational communities work together on reciprocal basis to develop globally accepted 6G standards. Moreover, digitalization is now modernizing many different vertical sectors. Therefore, it is in the clear interest of businesses that globally accepted standards and specifications will be developed for the digital products and services related to strategic European industrial sectors, e.g., the manufacturing, health, transport, energy, financial services, smart city and agriculture sectors in the 6G era.

To achieve the goal of 6G globally accepted standards several tangible and sequential steps must take place, such as:

- Establish cooperation with counterparts in other regions and vertical sectors by means of MoUs and joint events for information exchange and alignment of research work programmes.
- Maintain and further develop the global standardization ecosystem to cooperate towards globally accepted standards for the benefit of end customers and industry for interoperability, economy of scale and minimizing cost.

2. ACHIEVING 6G TECHNOLOGICAL SOVEREIGNTY FOR EUROPE

According to [15], the term **technological sovereignty** is defined as: *"… the ability for Europe to develop, provide, protect, and retain critical technologies required for the welfare of European citizens and prosperity of businesses, and the ability to act and decide independently in a globalised environment*". According to the same source, this definition encompasses three key elements, namely:

- *"Technological – the development of European R&D competencies by maintaining a strong knowledge base, strong industry, and strong networks in the critical technologies.*
- *Economic – the achievement and preservation of a position of leadership in Key Enabling Technologies (KETs), the ability to turn R&D into market products, and having access to a diversity of resources along the value chain with the aim of reducing dependence on third countries;*
- *Regulatory – the development of adequate policies and standards to influence global regulation, standards, and practices that reflect European values."*

The definition of **sovereignty** does not include the following extreme positions: on one hand **autarky**, which means the economic independence from other countries, which would require no dependencies on goods, materials, manufacturing, services and deliveries from other countries and import and exports with other countries, and on the other hand, **heteronomy** like control by other countries.

These extreme positions are considered to be inefficient and unrealistic as they would be counter-productive for innovation, the economic prosperity and global trade. In the current document the focus is mainly on the technological element, acknowledging however that proposing key strategies cannot avoid providing also suggestions related to economic and the regulatory elements.

In [15], 6 **key enabling technologies** have been identified for the technological sovereignty of Europe. Among these, **Security and Connectivity technologies** are included as most relevant for SNS. Additionally, 5 challenges are identified namely: a) lack of resources/raw materials, b) dependence on non-European suppliers, c) digital skills, d) commercialization of research results and e) lack of joint action and coordination.

The current document focuses mainly on the last four challenges and tries to provide some guidance on the way forward.

It is worth noting that the discussion on technological sovereignty cannot be decoupled from the geopolitical context. In a globalized economy it is worth studying the weaknesses and strengths of each region to understand how global cooperation and supply chains are currently formed.

Table 1 provides a rough analysis of the critical dependencies in selected technology fields between the USA, Europe, China, Taiwan, Korea and Japan. Clearly, Europe is very strong in communication networks. However, it is very dependent in (high-end) micro-electronics, cloud technology and the platform economy.

It is no secret that the world is facing some significant geopolitical changes. Countries or regions openly target a certain level of sovereignty to implement co-dependency and to improve resilience. At the same time today's economy is strongly globalized, and modern big companies are naturally multinational and active across many regions. A diversity of sources achieved as a combination of own capabilities and trade seems to be a viable way to achieve resilience. This resilience is also desired so that European values on regulatory aspects such as security, privacy, lawful interception, competition law, net neutrality, etc., as well as policies related to climate change, sustainability, and inclusion are implementable.

Table 1: Rough comparison of selected technology fields between global regions

Technology Sector		Europe	USA	China	Taiwan	Korea	Japan
Micro-electronics 1)	Design	Need to catch up in chip design	Dominance in chip design	Need to catch up in chip design	Weaker position in chip design	Strong position in chip design	Strong position in chip design
	Manufacturing	Strongly reduced capacity in manufacturing with 9 % in 2020	Strongly reduced capacity in manufacturing with 12 % in 2020	Strong growth of capacity in manufacturing with 15 % in 2020	Stable capacity in manufacturing with 22 % in 2020	Relative stable capacity in manufacturing with 21 % in 2020	Slightly reduced capacity in manufacturing with 15 %
Cloud technology and services 2)		Strong dependence from US vendors, only about 6 % market share	Strong dominance by US enterprises with about 70 % market share	Local supplier in China with until today small offers in Europe	-	-	-
Telecommunications infrastructure 3) **for 2018,** 4) **for 2019**		Leading two vendors with 30,4 % world market share	IT-supplier with 12 % world market share	Leading vendor with 37 % world market share	-	Supplier with 8 % world market share	-
Platform economy 3)		Weak position with only 3 % world market share	Dominant supplier with 70 % world market share	Strong position with 21,4 % world market share Focus on China	-	3,8 % world market share	0,16 % world market share

1) Boston Consulting Group, Semiconductor Industry Association: Government Incentives and and US Competitiveness in Semiconductor Manufacturing. September 2020, https://www.bcg.com/de-de/publications/2020/incentives-and-competitiveness-in-semiconductor-manufacturing.
2) Der Kinsta-Blog: Cloud Marktanteil – ein Blick auf das Cloud-Ökosystem im Jahr 2020. 29. Juli 2020, https://kinsta.com/de/blog/cloud-marktanteil/.
3) EU Kommission: „Industry Policy after Siemens-Alstom". 2019, file:///C:/Users/dems1cf8/AppData/Local/Microsoft/Windows/INetCache/IE/NLQHX0PI/ES0419287ENN.en.pdf.
4) Dell'Oro Group: Worldwide Telecom Equipment Revenue. https://www.delloro.com/key-takeaways-the-telecom-equipment-market-1h20/.

From the above table, it is clear that although Europe currently has a strong position in telecommunications, an analysis is needed of how European strengths can be maintained and developed, especially towards 6G. For example, the SNS JU aims to keep industry in Europe at the forefront of development and to catchup in areas, where Europe is behind. The following sections analyse several of the abovementioned domains and offer concrete recommendations.

2.1. COMPONENTS AND MICRO-ELECTRONICS

The **Horizon 2020 COREnect project** [16] has developed an industry roadmap to improve the European technological sovereignty in the microelectronics domain. The proposed industry roadmap is publicly available in the COREnect Deliverables D3.6 [17] and D3.7 [18].

The COREnect project investigated the following sectors by means of SWOT (strengths, weaknesses, opportunities, threats) analysis:

- Automotive grade connectivity,
- Infrastructure connectivity,
- Industrial grade connectivity and
- Consumer grade connectivity.

In the SNS context especially the infrastructure connectivity is of interest. The expert group proposed several concrete short-term, medium-term and long-term strategic actions to address technological sovereignty [18].

It is worth noting that in January 2023 a new **EU funded project called COREnext** [19] has started its R&I activities. The Project brings together expert stakeholders in future mobile networks and integrate their perspective in key focus areas like digital, analogue and integrated solutions for computing communication and sensing. The consortium is expecting to develop a trustworthy-by-design platform based on a new computing architecture for base stations to push European capabilities in B5G/6G to the next level.

The new **IPCEI (Important Project on Common European Interest) on Microelectronics** is currently in the pre-notifications phase in 20 participating EU Member States and the notification phase by the EU Commission. Its main objective is to invest in Innovative industrial capacities such as "critical raw materials, equipment, wafers, research, pre-production and design to support Europe's leadership in critical supply gaps and enabling innovation" [20]. This activity is related to the EU Chips Act to reduce dependencies and to improve resilience in areas like processors for high-performance computing, specialised chips for AI and autonomous driving. Worth mentioning is the ambition to develop a pan-European chips design ecosystem to tackle the new challenges on transistors in a more than Moore approach, and on circuits architectures with increased security and trustworthiness. From the SNS perspective, a cooperation on requirements on 5G and 6G systems towards research and design on necessary future microelectronics components is envisaged to improve the European resilience. Moreover, it would be beneficial to identify similar synergies with national initiatives from Member States.

"**The European Chips Act,** adopted by the Commission early 2022 aims to enhance Europe's competitiveness and resilience in microelectronics technologies and applications, and help achieve both the digital and green transition. One of its objectives is to help Europe reach leadership in chips for digital connectivity infrastructures. Europe has a leading position in the global connectivity infrastructure market, while at the same time has strong dependencies on chipset vendors from outside the European Union. EU will mobilise more than € 43 billion of public and private investments and set measures to prepare, anticipate and swiftly respond to any future supply chain disruptions, together with Member States and EU international partners. The aim is to (i) Strengthen Europe's research and technology sovereignty towards smaller and faster chips, (ii) Put in place a framework to increase production capacity to 20% of the global market by 2030, (iii) Build and reinforce capacity to innovate in the design, manufacturing and packaging of advanced chips, (iv) Develop an in-depth understanding of the global semiconductor supply chains and (v) Address the skills shortage, attract new talent and support the emergence of a skilled workforce.

Entering the SNS era, the **SNS R&I Work Programme 2021 – 2022** [21] is contributing to European policies including microelectronic components and is providing preliminary activities in areas related to green radio technologies, wireless communication and signal processing, communication infrastructure technologies and devices and experimental infrastructures. In the SNS Work Programme 2023 – 2024 activities on microelectronics are extended according to [22] based on established European policies such as the European Chips Act (Microelectronic components).

A number of joint **activities between the KDT/European Chips Act and SNS** JUs are envisaged in their respective Work Programmes, with both constituencies being encouraged to participate in such calls. In particular, the SNS Joint Undertaking Work Programme for 2023-2024 includes strand "SNS-2023-STREAM-B-01-05: Microelectronics-based Solutions for 6G Networks" and strand "SNS-2024-STREAM-C-01-01: SNS Microelectronics Lighthouse" that aim to develop an experimental platform where solutions from the micro-electronics domain developed either in the context of Phase 1 SNS WP, or Horizon Europe Cluster 4, or the KDT JU will be validated in terms of performance and applicability for 6G networks. Therefore, solutions developed in projects funded under the current KDT focus topic could find their way into the afore-mentioned SNS topic.

The SNS JU is also monitoring and **strengthening its links with the closely related area of photonics**. In the SRIA of Photonics21 for 2025 onwards (currently under development) it is clearly mentioned that cooperation should be strengthened as the SNS JU is working from network and system level downwards, whereas Photonics21 works from device and sub-system level upwards. Potential areas of cooperation are optical wireless communication, advanced optical transmitter and receiver technology, next generation Terabit/s transceivers, optical switching systems, photonic integration as a combination of optical, radio frequency and digital radio systems and highly linear optical modulators or fronthaul and backhaul systems. Activities in the SNS JU and the 6G-IA can derive important component and device requirements and can provide relevant test environments for prototype devices resulting from Phototonics21 developments. A close collaboration ensures that network, system, and component developments go hand-in-hand. Meanwhile, it would be worthwhile for the SNS JU and Photonics 21 to synchronize their activities for a holistic approach necessary to reduce the environmental impact of next-generation networks, encompassing four research pillars: energy-efficient hardware, energy-efficient software, energy-aware network planning, and sustainable operation of the network infrastructure.

It Is worth noting that the **NetworldEurope** has recently provided a SRIA [23] and an accompanying technical oriented Annex [24] that provide a detailed analysis of all technical topics related to 6G networks including topics related to devices, micro-electronics and optical networks. The document also provides detailed lists of research challenges in the short-, medium- and long-term timeline. This document, along with the corresponding SRIAs from of the Electronic Components & Systems and Photonics21 should be analysed in a cooperative way among the involved communities and funding instruments to investigate and identify how the research directions and eventually results to be produced can be synchronized to achieve multiplier effects.

If used correctly, the above-mentioned instruments could act as the catalyst to bring together research and innovation European resources to contribute towards technological sovereignty in the areas of components, optical communication, and micro-electronics for 6G connectivity. The knowledge and skills to be created, will help boosting the European market and reduce dependencies from other regions.

Recommendations:

1. Synergies between related Horizon Europe partnerships and European Technology Platforms (ETPs) need to be further pursued.
2. Joint collaboration roadmaps in the 6G areas of baseband, RF and signal processing, radio front-end, antenna systems, as well as optical communication components among related partnerships for the next two years need to be further investigated. Such roadmaps should take into consideration the priorities of each funding instrument, and the plans of the private sector.
3. Synergies between related Horizon Europe partnerships must investigate how integrated, configurable and generic hardware platforms will efficiently support network virtualization. Research activities should target solutions that will eventually foster supply sources diversification and cluster risks and dependencies avoidance from very few dominating sources to improve resilience.

2.2. OPEN SNS SOLUTIONS

Open networks are networks built based on open, standard-based and programmable architectures requiring the integration of various data sources and services into unified and automated platforms. Open networks solutions should be developed adhering to the World Trade Organization (WTO) Technical Barriers to Trade Agreement (TBT) upon which the EU Standards 1025 directive is built on, like in today's well-established principles and procedures of international standardization.

Open networks, refer to open interfaces as well open network function definition. They both target for a hardware and software disaggregation that is part of the network evolution already reflected in market developments during 2022-2023. Open networks expect to bring the following benefits:

- More choices for operators and manufacturers to mix and match components from different vendors thus diversifying their dependencies. The realization of this diversity opportunity is also dependent on available choices and market concentration in up-stream markets e.g., virtualization software, semiconductors, etc.
- Greater automation and flexibility for operational efficiency in network roll-out,
- New possibilities for innovation,
- New opportunities for European market players. (e.g., near real-time (xApps) and non-real-time (rApps) applications)
- Using cloudification, disaggregation and modularization as enablers for simpler network operation and management and hardware reuse capability when replacing SW or HW vendors.

Open networks are currently investigated as a promising solution to support the constantly growing data traffic and the need for network densification, in a TCO (Total Cost of Ownership) optimized way. The development of open networks is a complex topic and there are important issues to be considered to the envisioned solutions. An indicative list includes:

- Higher integration complexity that renders configuration, operation and update a challenging process, while performance is not always easily met, resulting in that the TCO promise is yet to be proven (shifting Capital Expenditures (CAPEX) to Operational Expenditures (OPEX))
- An increased threat vector for the overall security potentially leading to more vulnerability in the networks that needs to be investigated and mitigated,
- Use of Open RAN architecture (e.g., O-RAN) does not mean not using proprietary components e.g., for Distributed Units (Dus) and Radio Units (Rus). Open Interfaces in O-RAN architecture may be realized by manufactures using proprietary software. Confusion remains between open source and open interfaces/architecture and more work is needed to clarify the possibilities and expectations, especially on open source software and whitebox solutions
- Over-standardization of networks carries the risk of reducing the perspective of opportunities for innovation on top of network solutions,
- Energy efficiency is not easy to achieve when integrating software and hardware products from various sources,
- Without careful planning and well-balanced solutions, these approaches may end up only replacing a strong European sector by non-European solutions that will threaten the desired European technological sovereignty.

Today, open networks appear to be a significant trend where multiple stakeholders at a global level are working hard to achieve the aforementioned benefits and address the aforementioned issues. Although no one could safely claim today where these efforts will lead, this area clearly has potential and should therefore be considered in current and future European research activities.

All the latest findings suggest that more effort is needed to better understand the pros and cons and find the right balance between open and purpose-built solutions, as well as gain further understanding over the depth of the promise that open networks can bring. Already in the first R&I Work Programmes of the SNS JU related activities have been planned both in long term research topics as well as in experimental platforms [21], [22].

However, additional research and innovation efforts and additional accessible experimental platforms are needed to reach widely accepted and well-balanced solutions. The following set of recommendations captures the key points for the way forward.

Recommendations:

1. Further strengthen a collaborative European research and innovation, environment for open SNS solutions where new results will progressively reach higher Technology Readiness Level (TRL),
2. Create pan-European large-scale testing facilities to transparently verify achieved results in terms of reproducibility, repeatability and reliability of claims,
3. Promote the engagement of European actors along the full chain to generate innovative solutions and services,
4. Develop a public marketplace of research and innovation facilities and solutions available to European stakeholders for experimentation and generation of new knowledge. Towards this end, it is important to leverage existing testing facilities and ensure linking and complementarity at a European level,
5. Reinforce European leadership in standardization for open networks,
6. Ensure that the provided solutions address security and privacy conforming to European values, EU standards and citizens' needs,
7. Build-up and retain a knowledge base of experts to implement, operate and manage Open SNS infrastructures.

2.3. CLOUDIFICATION AND DISTRIBUTED COMPUTING

Cloud infrastructures will play a crucial role in 6G. Already in the 5G era, applications are implemented in the cloud. With 6G this phenomenon will intensify using a cloud continuum from space cloud to terrestrial cloud and edge networks. In the 6G era applications will be implemented on cloud infrastructures, while the core and access networks will be cloud ready as well. One of the envisioned challenges is to come up with solutions that will run network functions in the cloud in the most energy efficient way.

Cloud infrastructures do not offer only storage but claim to offer best in class operational automation and AI/ML based optimisation and use cases, commonly purpose built (c.f., section 2.2 and 2.4). It is worth noting that there are still some challenges on cloudification, integration and lifecycle management.

In the case where both application providers outsource the hosting of their applications, and telecommunications operators outsource the hosting of their networks to cloud providers, there is a risk of a chain dependency. In addition, resilience is at risk. It may be that multiple telecommunication network providers and applications (e.g., an electricity distribution company) use the same cloud provider. If this cloud provider suffers from an outage, there will be widespread outages of digital infrastructures.

A way to address the dependency on cloud Infrastructures is to ensure Interoperability between cloud infrastructures. That way it is possible to have different independent cloud infrastructures that are separately optimised for a specific task or market. For example, there can be cloud infrastructures that are optimised for high-speed media/data processing in a telecommunications network; cloud infrastructures that are optimised for computing, edge/cloud infrastructures that are distributed to be nearby the end-users; or private cloud infrastructures implemented at factory premises. Such standardized interoperability can be used to further enhance the resilience for a specific market segment where more than one cloud operator could offer their solutions to specific customers. Technology development should address interfaces for cloud interoperability and should cater for specific performance optimization of cloud infrastructures for the transport of 6G user data in radio access and core.

During the development of 6G technology, it is important to take cloud sovereignty into account. This includes control and storage of data that will be under domains that are controlled or conform to EU jurisdiction and legislation. There are currently concerns in Europe about the low footprint on the provision of cloud infrastructures. From the perspective of sovereignty and diversification, the current situation is sub-optimal. This has pushed the EU and Member States to take measures aimed to reduce this dependency (e.g., GAIA-X[25], IPCEI-CIS [26]) . Additionally, in the context of the Horizon Europe, the European High-Performance Computing Joint Undertaking is targeted to provide secure cloud-based supercomputing services for a wide-range of public and private-users everywhere in Europe [27].

Very recently, the Sylva Open Source project [28] was started by five European telcos in collaboration with the main European vendors and under the auspices of the Linux Foundation Europe [29]. According to their white paper [28], the Sylva project has two main objectives:

1. To release a cloud software framework, which shall:
    - Identify and prioritise telco and edge requirements,
    - Develop solutions to the specific technical challenges identified on the infrastructure layer of the telco ecosystem,
    - Integrate these solutions with existing open-source components,
    - These solutions and the integrated cloud software framework are not "production ready" software, but aims to be "production grade" in order to be used by third parties such as operators, network function vendors, and cloud providers to create commercial products,
2. To develop a reference implementation of this cloud software framework and create an integration and validation program to:
    - Validate the commercial network functions against this cloud software framework,
    - Validate implementations based on the released framework and its components,
    - Accelerate commercial adoption of network functions and their compliance with this cloud software framework.

According to the Sylva project FAQ [30], the first commits are expected in 2023. A first version of the cloud framework is expected to be released in mid-2023.

Recommendations:

1. Stimulate innovative European solutions that address the need for network cloudification in all domains (RAN, edge, core),
2. Exploit and enhance open-source solutions to contribute to 6G technological sovereignty,
3. Develop open interfaces to enable cloud interoperability, cloud enabled telco services interoperability
4. Prioritize European solutions that conform to European values, legislation for data security and privacy,
5. Implement EU-based open, interoperable, and multi-provider cloud infrastructures for ICT networks.

2.4. NETWORK INTELLIGENCE

It is widely accepted that Artificial Intelligence (AI) will be of paramount importance in 6G networks connecting human, physical and digital worlds ([31], [32]) and may be a huge opportunity to provide advanced AI based services using network supported functions and/or network generated data. As presented in [33], AI and ML (Machine Learning) will be an integral part of the system network architecture with AI services and applications being highly intelligent and autonomous. As shown in Figure 2, AI and ML are expected to assist in almost all technological areas of operation of 6G networks. To secure AI systems throughout the entire machine learning lifecycle, confidentiality, integrity and availability must be ensured to keep the model confidential and secure. In addition, AI systems should be designed to preserve data privacy.

AI, digital twins and other intelligent components will also be an integral part of services and applications that will need to be supported by 6G infrastructures. In turn, they will also be supported via native AI parts of the 6G network. Many of these intelligent components will be provided within the 6G infrastructure (e.g., they are provided on edge locations or require specific network support). To allow interconnection and interoperation of intelligent components across different stakeholders, open solutions and carefully selected standardised interfaces are needed.

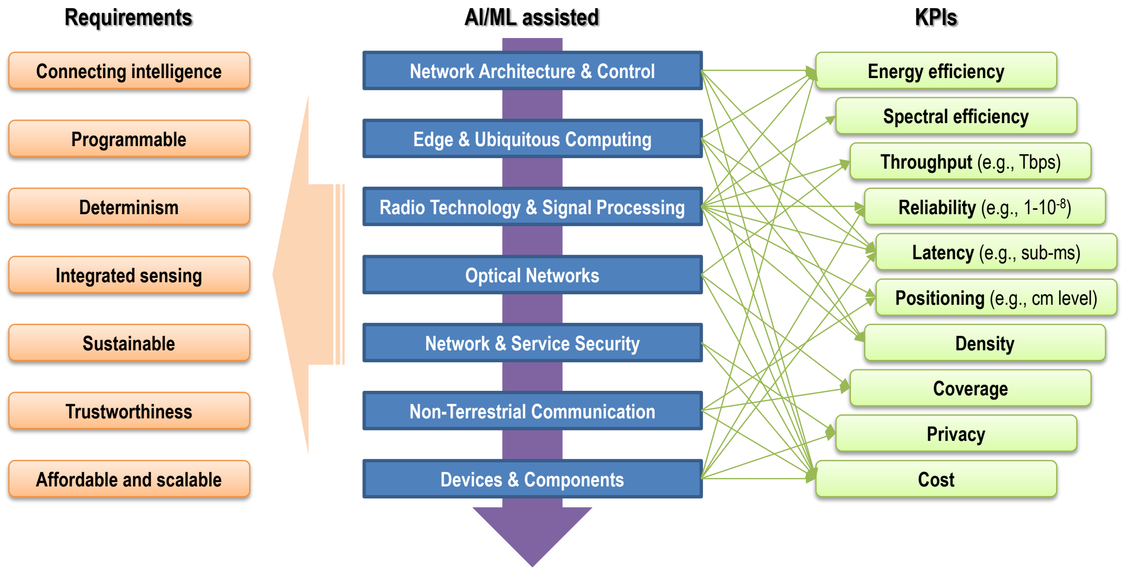


Figure 2: Technology areas with strong impact on different 6G requirements and KPIs [14]

This reality has been captured from the beginning in the preparation of the SNS JU proposal [1] and in the subsequent SNS JU Work Programmes [21], [22]. In the context of the SNS JU, AI/ML solutions have already been identified in various streams ranging from long-term research activities to experimental platforms and large-scale trials. Notably in the *HORIZON-JU-SNS-2023-STREAM-B-01-06*: *EU-US 6G R&I Cooperation AI solutions* and the *HORIZON-JU-SNS-2024-STREAM-B-01-08*: *Reliable AI for 6G Communications Systems and Services* may be considered at various levels from a future target 6G system, from lower layer radio aspects to higher layers targeting intelligent function placement, network self-configuration, security and resilience, or AI based support of user applications. This call also targets the support to a reference framework for AI usage for the telecommunications domain in relation to 6G, including methodologies, reference use cases, data acquisition and generation, repositories, curated training and evaluation data, as well as the technologies and functionalities needed to use it as a benchmarking platform for future AI/ML solutions for 6G networks.

At the same time, a significant number of global research efforts as well as related standardization activities are progressing to provide results for Beyond 5G and eventually 6G systems. A comprehensive survey can be found at [34], where a detailed analysis of 5G PPP activities is presented, together with a summary of standardization activities, a list of open issues and a set of recommendations.

Based on the findings of the aforementioned white paper and the previous analysis it is clear that for enhancing future network return of investment the following areas need further attention (research and development work):

Recommendations:

a) Define and implement standardized interfaces for training and execution of AI models
b) Ensure that either real-world or synthetic datasets for training purposes are available for use in SNS and promotion of such datasets towards standards bodies for system benchmarking and evaluation.
c) Run pilots with new customer segments to identify AI/ML opportunities
d) Examine the use of AI/ML and automation for network operations, including control and management functions, in a sustainable way
e) Stimulate adoption of new solutions for AI/ML and automation to facilitate the introduction of new use cases and services,
f) Establish and ensure long term operation of an open repository for communications and networking datasets that can be used for training and benchmarking AI/ML algorithms,
g) Define widely accepted data acquisition and curation procedures that with a strong impact in standardization activities,
h) Develop synergies between SNS JU and AI, Data and Robotics cPPP.
i) Define open solutions and standardised interfaces that enable interconnection and interoperation of intelligent components across different stakeholders.
j) Secure AI systems throughout the entire machine learning lifecycle.

2.5. SECURITY AND PRIVACY

Security is one of the first fundamental rights [35] and a pre-requisite for strategic autonomy as a policy objective of the European Union in a cyber-physical world. The economies' reliance on digital infrastructures drives stringent requirements on our ability to ensure secured development, including relevant supply chains, deployment and operations of 6G technologies and reducing Europe's overall strategic dependencies. There is a direct relationship between the ability to provide and master the technologies along their full life cycle and the implementation of security policies. Those policies are in turn the enablers for conformance with regional values and legal framework.

The European Union is leading the perspective of a global resilient human-centric digital era and develops positions and policies for that purpose (e.g., NIS2, CRA, AI act, etc. [36] – [40]). This may be an opportunity to leverage better resilience for the entire society including critical vertical sectors and better chances for societal acceptance with respect of fundamental values such as privacy. The recent General Data Protection Regulation (GDPR) experience shows that while fragmentation of legislations and standards between regions are in general detrimental for the industry, well-defined policies can be beneficial, showing digital maturity and gaining global momentum.

Beyond mandatory "by design" approaches for each and every component of the 6G architectures the intrinsic dynamic End-to-End nature of security mandates to address its complex time and space dimensions/challenges with a holistic view. Below we analyse 4 main pillars related to security and privacy.

A. Identification of threats

Threats – thus the strategic impacts – are the combination of the expected security level, sophistication of malicious attacks, attack surface/vulnerabilities of the technologies, systems and services and remediation capabilities. Ongoing European cooperation with ENISA on 5G (threat landscape [41], Tool box [42]) may be extended with a **6G-dedicated cooperative European Cyber Threat Intelligence (CTI)**. Joining public and private forces (Computer Emergency Response Team – CERT, Computer Security Incident Response Team – CSIRT, Security Operating Centre – SOC), on multiple technological areas such as security, telecom, cloud, IoT, space, etc.is key to distribute and share security knowledge among the wider stakeholder landscape. One of the virtuous consequences of such an approach will be to anticipate at this stage the applicability of European policies.

Europe should be able to provide solutions that will conform to the European legislation. As identified in section 2.3, Europe needs to have a clear strategy for cloud services. Towards this end, activities considering open-source building blocks used for a cloud continuum infrastructure (from far edge to hyperscalers) appear to be a promising answer for European stakeholders.

A second wide area policy-related field is the evaluation & monitoring of security conditions where past approaches of certification (already complex to unify) are even more challenging considering flexibility of the systems and distribution of control/liability perimeters.

B. Protection

Policies about protection encompass multiple angles of 6G. In this context, the definition of sovereignty provided in Section 2 of this document applies, which emphasizes that the definition of sovereignty and its realisation does not include (1) autarky (or protectionism) and (2) heteronomy. Focusing on policy-dependent items we can list:

- Data centric issues: confidentiality, privacy, cryptographic requirements (Post Quantum Cryptography), localisation of storage, processing, applicability of legal framework, root of trustable AI, etc. 6G is about communication but also about inter-computing connectivity and can't be agnostic to these issues. One can differentiate at least three types of data, namely: a) users' payloads, b) 6G control and management data, c) behavioural/localisation extracted data from 6G systems and services usage.
- Hardware and software components: It may be worth here to give a focus on supply chains as explained in section 2.1. The goal for Europe should be to ensure that blocking should not occur in the supply chain which is a dependency chain, nor there should be question marks on the certification of hardware products. Specific attention to HW/SW security functions/components is key to master the 6G infrastructure and services.
- Software defined operations: Security is a living matter which must follow the variance of the system, the software defined operation must be done both in a resilient way respectful of requested policies. With an immediate impact on liabilities, transparency and forensic may be considered as part of the new challenges. It is also an area where **integration of security Services** (Managed Security Service Provider – MSSP) should globally benefit to all players.
- End-to-end solutions: Finally, 6G will accelerate the service dimension. Here, linked to evaluation challenges, the goal should be exposure of security attributes qualifying sub-systems and (micro)service components. This is a challenge to **enable End-to-End service composition and Users' awareness of Digital usages**.

C. Detection & Response

Smart counter measures against attacks obviously mandate to detect the attacks.

- Means to detect (e.g., Extended Detection and Response – xDR functions) should be generalized or even mandatory (this is already the case in some regions) for essential services.
- Contamination or just correlation of attacks leads to a need of cooperative approaches. Although linked to the CTI proposal above, collaborative structures may be developed for the wide 6G communities, from basic 6G service users, verticals and Non-Public Networks users, up to large telcos and service providers.

D. Resilience and Recovery

The last phase of Cyber security, recovery, has many aspects related to resilience. Learning from experience, feeding the CTI, improving process and remediation, is coming in addition to previous statements at a different time scale but claiming for continuous 6G security. Challenges raised by 6G technologies and its expected contribution to societal and economic dimensions mandates to master its security and privacy. Based on a valuable policy maturity, our industry has an opportunity to drive 6G for the better, enable its trustable development/deployment and generate subsequent growth.

It is worth noting that NetworldEurope has identified a detailed list of topics for further research and innovation activities [24]. Moreover, the Smart Networks and Services has already defined the necessary axis aiming at contributing to the numerous challenges' solutions [21], [22].

Recommendations:

1. Create a collaborative environment for key public and private forces that are actively dealing with security and privacy to work together and cover the complete range of needs from research activities, opportunities for new products and services as well as policies
2. Identify areas where critical hardware and software solutions are indispensable and ensure European implementations of such solutions,
3. Develop and adopt certification processes for hardware and software solutions so that their conformance evaluation against European policies and legislation is feasible without impacting access to critical ICT technology for Europe.
4. Develop synergies and joint actions between 6G-IA and ECSO including on standardization, certification and labelling.

2.6. SNS KNOWLEDGE BASE & SKILLS

As mentioned in [43], "Europe is lagging behind with its digital talent in the current scenario" while [44] clearly mentions: "The EU's 9 million ICT specialists also fall well short of the EU aim of 20 million specialists by 2030 and are not enough to address the skills shortages that businesses, SMEs and organisations are now experiencing, despite the fact that 500.000 ICT specialists entered the labour market between 2020 and 2021.

The 2022 results demonstrate that while the majority of Member States are making progress in their digital transformation, essential digital technologies like AI and Big Data are still not widely used by enterprises. The deployment of connection infrastructure, particularly 5G, which is necessary for highly innovative services and applications, must come quickly."

Moreover, it is important to promote equality, diversity and a gender balanced approach in the 6G R&I community and working environment. Women need to be encouraged joining into technical and engineering studies and actively participate in the European 6G R&I community, as currently the sector is missing a significant part of experts.

The EC has recognized the Importance of creating a knowledge base and takes measures towards addressing these challenges for Europe [45]. Thus, there are possibilities through a coherent Horizon Europe Programme to stimulate the creation of appropriate actions that will enable European talents to build their skills on key 6G technologies (e.g., AI/ML, cybersecurity, IoT, advanced RAN, transport and core connectivity solutions, etc.).

The 6G-IA has already mobilized a critical mass of European stakeholders that are active working in innovative 6G solutions for smart networks and services. Also, At the same time the SNS JU is offering a unique opportunity to create a 6G SNS knowledge basis supported by a plethora of experts. Thus, it will be of paramount importance to come up with concrete steps to take advantage of such opportunities and integrate them with the European educational framework.

Finally, Women in Telecommunications and Research (WiTaR) is an EU-level initiative that promotes gender equality, inclusion and empowerment in the 6G Research & Innovation (R&I) community. This initiative was originally established by Hexa-X as Women in Hexa-X initiative in February 2021 and then it was expanded for the participations of the whole 5G PPP community in June 2021. Currently, this initiative operates as a 6G-IA WG.

1. Ensure that the generated knowledge becomes an integral part of the curricula in Europe, starting with the SNS calls from 2025,
2. Collect the generated knowledge on 6G smart networks and services and make it widely available for European experts in life-long learning activities
3. Stimulate and motivate 6G-IA members to support the skills development through open lectures on key topics.

3. TARGETING SUSTAINABILITY

In 1987, the United Nations' Brundtland [46] report defined sustainability as "***meeting the needs of the present without compromising the ability of future generations to meet their own needs [47]***." Today, worldwide efforts are seeking ways of meeting their development needs, but with the increasing threat of climate change, concrete efforts must be made to ensure development today does not negatively affect future generations.

Sustainability is a societal goal that is usually addressed under three pillars, namely environmental, economic and social. A related concept that many times is used as a synonym is that of the sustainable development. The UN SDGs refer to the pathways and needed action to achieve the long-term target of sustainability.

The 2030 Agenda for Sustainable Development and the related UN SDGs [48] aim to strengthen the social, economic and environmental dimensions of sustainable development. Beyond these objectives reinforced by the European Green Deal [49], which sets out a target for the EU to achieve climate neutrality by 2050, research on Smart Network and Services needs to address how 6G will be sustainable and how it will contribute to the sustainability of other sectors.

Sustainability is increasingly becoming a key target for the design of 6G, driving the choice of technologies and conception of the system to reach effective 6G solutions, with reduced environmental impact. Sustainability per se is a worthwhile target. However, the challenge is how to move from slogans into concrete actions to make it happen.

The European Green Deal [50] provides a roadmap for making the European economy sustainable by turning climate and environmental challenges into opportunities across all policy areas and making the transition just and inclusive for all.

While the main ambition is to ensure that Europe will be the first climate-neutral continent by 2050, the set of target objectives aims on developing and ensuring a *"new growth strategy to transform the EU into a fair and prosperous society, with a modern, resource-efficient and competitive economy where there are no net emissions of greenhouse gases in 2050 and where economic growth is decoupled from resource use".*

For attaining the sustainability goals of the Green Deal in many different sectors, the EC has anticipated the need to invest on digital technologies such as **Artificial Intelligence, 5G and 6G, Internet of Things, Cloud and Edge computing**. Such technologies offer new opportunities for effective sustainable solutions. At the same time, the Green Deal underlines also the need to investigate and invest in ICT technologies that are more sustainable (greener / more energy and climate friendly) by design.

Recognizing the need for sustainability the SNS JU has acknowledged the work currently performed under the 5G PPP Initiative [51] and has identified related topics in various streams and strands in the SNS JU [21], [22]. Moreover, there is already a plan to organize a call for a sustainability lighthouse project that will bring the multiple solutions together and provide a clear European answer for sustainability.

The work covers both "Sustainable 6G" and "6G for sustainability". It includes identification and developments of the technology/architectures needed to make 6G solutions (end-to-end) sustainable. "Sustainable 6G" and "6G for sustainability" should be considered with equal importance. Sustainability will be considered through three dimensions: (i) environmental sustainability, targeting the minimisation of environmental impact; (ii) societal sustainability, aiming at providing value to people and society thanks to new use cases powered by 6G, and (iii) economic sustainability, where 6G will be an enabler for business value. This threefold approach will drive the design and integration of technical solutions into an end-end sustainable set of tools and solutions. These three dimensions are briefly analysed in the following subsections.

3.1. ENVIRONMENTAL SUSTAINABILITY

As mentioned in [52], "there is a growing public awareness of environmental sustainability and the impact of technologies on energy consumption and usage of natural resources. Regulators are addressing the carbon footprint of networks and their related usages". The document provides references to several activities taking place in Europe both at national and EC level.

In the framework of 6G networks, the environmental sustainability aims to minimize the environmental impact, i.e., to reduce the consumed energy and the carbon footprint of manufacturing and operation of 6G networks but also to decrease the environmental impact of other industries (textile, automotive, food, pharmaceutical, etc.) by enabling disruptive services to digitalize and optimize processes. In other words, 6G should cater for sustainable 6G networks as well as 6G for sustainability on all sectors that it will be used.

Possible key sustainability objectives are (1) the specification of applicable environmental sustainability indicators, (2) methods for evaluation and (3) their application and use to connectivity solutions, including 6G. One approach that is expected to be followed in this context, is the calculation of the net avoided emissions in the industrial sectors when ICT is used. Globally accepted indicators and models for environmental sustainability should be developed for connectivity solutions including 6G. Specific recommendations and an overview on methodologies for assessing Carbon Footprint are provided, e.g., in [53].

To address sustainability requirements, research on future networks and services needs to be driven by environmental-related targets which notably embrace technology energy efficiency, sustainable services and equipment including terminals, and end to end CO_2 reduction in the entire value chain [54].

Large efforts must be invested buy all parts of the ecosystem. Industrial stakeholders need to reduce their carbon footprint by extending the hardware lifetime (while implementing modularity and reparability) and by including efficient transportation and recycling processes in their products. They should also find ways to minimize the energy consumption in their operations. Service providers aim to implement new sustainable connectivity technologies, extending infrastructure sharing principles, enhancing services for energy-free devices [55], or even streamlining network traffic and limiting electromagnetic field exposure.

The challenge is that 6G aims to support enhanced services (internet of senses, immersive environments XR/VR, digital twins, holographic type communications, smarts homes and cities) requiring huge data rates while reducing the required total energy per transmitted bit. In fact, due to the expected traffic growth, decreasing energy consumption is very ambitious, even when previous generations have showed that energy is reduced by a factor of 10 at each evolution. In 6G, when considering the capacity gain, the goal is to find the required trade-off and balance between performance and sustainability goals.

Since a low environmental impact relies on minimizing both consumed energy and emitted CO_2 during operation of 6G networks but also during the lifecycle of network equipment and terminals (from raw material, manufacturing, transportation, maintenance, up to recycling in end of life), automating energy consumption optimization will likely become mandatory in all network segments and during every stage of 6G lifecycle. Automation can be achieved by a smart closed loop which includes monitoring, AI-based analytics techniques, and modification actions to fulfil the required performance and energy consumption requirements without impacting the quality of service. Techniques to reach zero consumption at zero load (when no data is transmitted) need to be investigated for each 6G physical or virtual component. 6G needs to go beyond advanced sleep modes of radio access units and to implement auto-optimized smart components in terms of energy throughout the end-to-end network.

Besides energy optimization, resource sharing principles could be also investigated in 6G, including research activities to identify additional sustainable solutions. Embedded resource sharing functions are challenging when conceiving new 6G components and protocols. The sharing principles which can be applied at all layers include both hardware and software components, and give rise to new actors, for instance tower companies, cloud owners, among others; the target is to extend capacity but not the equipment. Multi-operator or even multi-actor (including cloud industries, IoT dedicated companies, private network owners, etc.) platforms and networks particularly require advanced end-to-end management and orchestration mechanisms. When various actors are involved in an end-to-end service, trust aspects need to be addressed to guarantee the required quality of service for users, thus, specific trust mechanisms need to be envisaged to enable sharing agreements between the parts or even the implementation of a dynamic marketplace. (A trustfulness model based on distributed ledger technology is proposed in [56]).

An energy-aware approach relies also on both access agnostic and hardware agnostic networks. Enabling transparent handover among WiFi-based, satellite-based, or 6G-based access networks can significantly optimize energy consumption while increasing resilience and coverage. For example, handover can be performed under both “best connection” and “energy efficiency” principles. Better network performance can also contribute to optimal battery consumption in terminals. Moreover, instantiating cloud-native network functions on commercial off-the-shelf servers appears to offer some promising solutions for the implementation of sharing principles as well as to avoid manufacturing and deploying dedicated hardware, which shall contribute to sustainable 6G networks.

As mentioned earlier, striving for environmental sustainability may have conflicting goals compared to those of other sustainable pillars and technological sovereignty targets. For example, there are arguments that optimizing for cost in terms of open/multi-vendor/multi-actor networks and optimizing for other values such as energy performance could be a challenge as an open cloud native network may consume more energy. This is why more research and innovation activities are needed to draw concrete results and ensure that the best-balanced solutions will be eventually followed by the industry.

3.2. SOCIETAL SUSTAINABILITY

Societal sustainability is of prime importance to several UN SDGs. It encompasses several areas such as safety, security, trustworthiness, and inclusiveness. As mentioned in [52], “societal requirements should be considered with equal importance as performance requirements”. Societal requirements may include higher EMF-awareness, higher digital inclusion (with improved affordability, coverage of low-density areas), higher security and much higher resilience.

What is still missing, is a well-defined framework that will assist a proper and concrete methodology to evaluate 6G solutions and how these contribute to fulfilling societal requirements. A possible way forward to address this challenge is described in section 3.4.

Research activities to provide solutions for societal sustainability are required. The SNS JU has recognized this fact and has integrated this priority in the SNS R&I WPs [21], [22]. Currently a dedicated call for sustainability is being designed in the context of *HORIZON-JU-SNS-2024-STREAM-B-01-07: Sustainability* by providing among other things societal sustainability, aiming at providing value to people and society thanks to new use cases powered by 6G. Moreover, the call on *HORIZON-JU-SNS-2023-STREAM-CSA-01: SNS Societal Challenges* is targeting to identify why society needs 6G solutions and consider the acceptability of a new 6G technological wave, as well as potential effects at societal and environmental levels and on public health.

These policy objectives are a clear direction for the European stakeholders to work on solutions that will address societal needs along the typical and well-needed technological breakthroughs.

3.3. ECONOMIC SUSTAINABILITY

The telecom sector is vital for the European economy and pivotal for the green and digital transition. The sector generated 4,5% of European GDP (2021) with a contribution amounting to 760 B€ of economic value added, supports 2,6 million of jobs and produces 109B€ of public funding (taxes). It is expected that by 2025 the telecom sector will add 840B€ of economic value and 20 million new mobile internet subscribers [57], [58].

540B€ of economic value added are productivity gains that will be further boosted based on the needs from verticals that require smart network and services as a flexible “connectivity platform” that will operate as an integral part of their business process. The challenge for Europe is to mobilize the critical mass of stakeholders to support this business transformation, avoid fragmentation and enable early adoption of solutions, filling the gap of 5G coverage with respect to other regions of the world and enabling a fast take off for 6G in 2030.

At the same time the telecommunication market is facing its own challenges. The European telecom sector has invested 500 B€ [59] in the last 10 years and will need 42B€ of additional investment (on top of private expected investments) per year to reach 2030 Digital Decade targets [60]. To trigger additional private investments, the policy measures, established 20-30 years ago in a very different socio-economic environment, are now being revisited encompassing different dimensions.

Towards this end research and innovation activities for 6G networks should focus on solutions like adequate support for network cloudification and fostering distributed computing infrastructures for Europe. Moreover, innovative frameworks that will enable cost reduction and simplification of network and services deployment [61] need to be developed. These frameworks should offer innovative solutions in areas that are desirable to make 6G technologies more acceptable by the public (e.g., EMF).

Technological breakthroughs are needed to support supply-chain diversity to improve network security and resilience by finding the right balance between disaggregation and greater interoperability while ensuring network performance, high level of security and sustainable levels of energy consumption.

Finally, new policy frameworks are needed that will boost the regulatory authorities to simplify deployment by considering reasonable spectrum licencing conditions, fair allocation of costs for network traffic and ways to stimulate data-driven technologies and services [62].

3.4. KEY VALUES INDICATORS

As mentioned in the previous sections, 6G should be designed not only for performance but to have a positive impact on societal values, and most critically for sustainability. Ambitions related to societal values point at the need to consider value-related goals and expected impact, which can be assessed with Key Value Indicators (KVIs) in relation to the usage of 6G networks. This value-related view should complement performance-related capabilities, assessed with Key Performance Indicators (KPIs) in relation to the design of 6G networks. Currently, at a global level an agreed framework to evaluate KVIs is not in place. Without such a framework it will be impossible to properly compare technological solutions and reach a unique set of standardized solutions.

The use of KVIs Is a tool to demonstrate the value impact of technology and how societal challenges are addressed. Value-related goals and expected impact need to be defined in a way that clarifies their relation to specific values, considering the enabled effect and design of 6G networks.

Key Values (KVs) are values important to people and society that may be directly addressed or indirectly impacted by future network technology, and to specifically be considered for 6G. The UN SDGs provide a well-established framework for societal needs and values, which serve as a good starting point in covering economic, societal, and environmental sustainability. In addition to the UN SDGs, values such as privacy, digital inclusion, and trust should be highlighted.

A KVI should be a measurable quantity that in some form provides an estimate of an affected KV. The formulation of KVIs should be done together with experts in the relevant field to ensure their relevance. Evaluation of KVIs can be done in several steps: a first-guess assessment, an assessment through expert consultation/user panels; simulation / emulation; and finally, a measurement/evaluation after deployment of the use case.

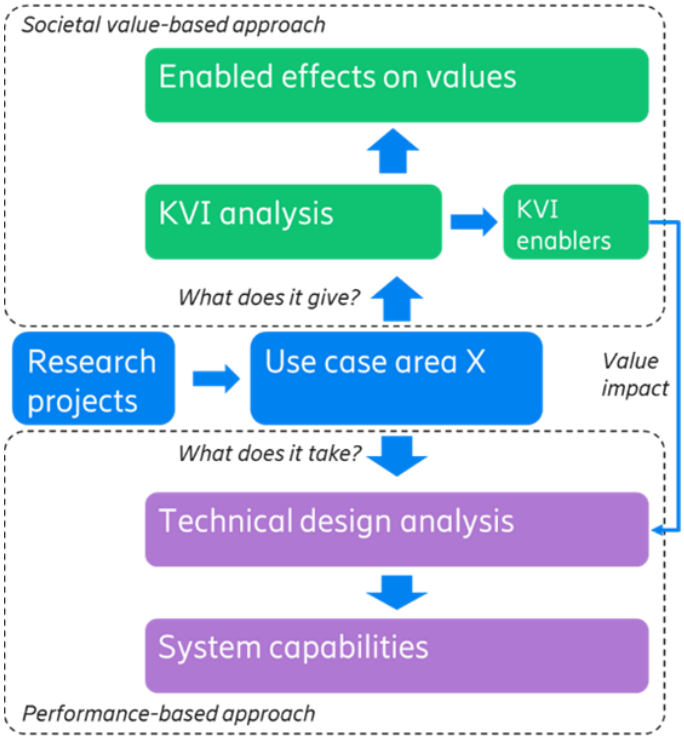


Figure 3: KVI analysis based on Use cases

KVs and KVIs are related to the usage and proliferation of network technology through use cases and is a societal value-based complement to the performance-based development [63]. This is illustrated in Figure 3.

As is discussed above, it is useful to make a distinction between Sustainable 6G (direct sustainability impact) and 6G for sustainability (the enabled effect from network usage). Sustainable 6G can be assessed in terms of KPIs, e.g.:

- Energy consumption of networks

- Resource usage (materials) for networks hardware, e.g., measured as CO_2 equivalents

To understand the enabled sustainability of 6G networks, 6G for sustainability, one needs to study the impact on use cases that are relevant for the values represented by the SDGs and other KVs. This impact should be estimated with quantitative measures (KVIs) that are both relevant for the KV in question and relevant for 6G network usage. Formulation should be done in a collaborative effort between experts in the value domain and in the telco domain. Some examples of this approach are given in Table 2.

Table 2: Key values mapped to use case areas and related KVIs

Use case area	KV examples	KVI examples
Emergency response & warning systems	***Societal sustainability***	*Reduced emergency response times; Increased operational efficiency of interventions in remote areas*
	Environmental sustainability	*Increased area of protected and surveyed natural habitats and climate preserves*
	Trust	*Reported confidence in advanced digital devices, systems, and services in critical missions*
Smart city with urban mobility	***Environmental sustainability***	*Environmental footprint of urban transport of persons and goods*
	Personal health and protection from harm	*Injuries in urban traffic*
Personal health monitoring & actuation everywhere	***Privacy and confidentiality***	*Reported user control of medical data for storage/transmission/processing*
	Societal sustainability	*Average cost saving in health care system per patient*
	Trust	*Reported trust level for autonomous e-health components; Accuracy rate in e-health AI-related events' identification and/or decision making*
Living and working everywhere	***Societal sustainability***	*Travelling / commuting time reduction; Access to job market; Life opportunities in rural areas*
	Economical sustainability and innovation	*Cost-efficiency of living and working in rural areas; Number of activities that can be performed anywhere*
	Digital inclusion	*Access to internet in communities and areas*
Sustainable food production	***Environmental sustainability***	*Environmental footprint of agriculture activities; Energy use in agricultural activities*
	Societal sustainability	*Increase in agriculture productivity; Reliability of food production*

Concretely, the KVIs will be a comparison between the impact without 6G and the impact with 6G. Given the high uncertainties involved, the impact can be labelled e.g., as "low" (<10% impact on a KVI), "medium" (10-50% impact on a KVI), and "high" (>50% impact on a KVI).

The outcome of a KVI analysis should then be a score list of expected value impact per use case. This KVI score adds another perspective to the performance score, and a possible trade-off between the two perspectives can then be discussed.

Recommendations :

1. Further develop the KVIs methodology as a framework to quantify and evaluate sustainability related breakthroughs (all solutions must target sustainability, so all solutions must be ready to be evaluated against the key European values)
2. Promote the KVI methodology, initiated by Hexa-X and to be further developed under the 6G-IA Vision WG to standardization bodies
3. The double perspective of performance goals vs environmental, societal and business value impact should be taken into consideration when developing new technologies

4. CONCLUSIONS AND NEXT STEPS

This document provides a comprehensive set of key strategies for 6G smart networks and services, capturing the views and priorities from the members of 6G-IA. The focus of the first version of this document was on specific aspects for technological sovereignty and sustainability. The goal was not to include a complete list of topics but kick-off the discussion on several important topics related to the development of 6G smart networks and services. Already it offers concrete recommendations on the various areas and how these can be implemented through 6G-IA actions and considered for inclusion on future versions of the SNS JU SRIA and R&I Work Programmes.

To complement this, and anticipate further work and position development, the implications of the above-mentioned stated policy directions will be further investigated. In particular, the implications on the service provider ecosystems will be addressed. At this stage we merely observe that the public communication service providers (aka. Telcos) are today offering fundamental public communication services founded in interoperable and federated multi-stakeholder platform ecosystem capabilities (built upon public interconnected networks and services). These offerings have not been substantially evolved over the last couple of decades. The so-called Telco Voice, SMS/MMS, and the Internet Access Service for best-effort Internet connectivity remains as the fundamental service offerings and the inherently interoperable multi-stakeholder platform capabilities have been from this high-level perspective rested at a status quo. The reasons for this are multi-faceted and deserve more attention. On the contrary, there have been huge developments of single stakeholder platform ecosystems and offerings, including a vast portfolio of

Internet applications enabled by the above communications platforms.

Hence, in the further work and policy position development the potential evolution of such multi-stakeholder platform ecosystems will be addressed. We anticipate several main areas of further innovations and developments that all will require open, standardized APIs and "as a Service" thinking, to enable efficient and automated inter-operator interaction and new service offerings. This will be both at the wholesale and the retail level, and from a local and national level as well as at the international level. The anticipated directions will likely consider separation and interaction between the main "layers" briefly identified in the current document as infrastructure, connectivity, compute, and application layers. However, the further development of such multi-stakeholder platform offerings are significantly harder than the cases of single-stakeholder platforms. Further developments of multi-stakeholder platforms are more complex and require multi-stakeholder alignment and incentive compatible solutions and business models. Supporting policies will be important to move such service provider ecosystems forward.

REFERENCES

[1] Smart Networks and Services (SNS): Draft proposal for a European Partnership under Horizon Europe Smart Networks and Services. 30 June 2020, https://research-and-innovation.ec.europa.eu/system/files/2020-07/ec_rtd_he-partnership_smart-networks-services.pdf.

[2] Council Regulation 2021/2085, Available at: https://eur-lex.europa.eu/eli/reg/2021/2085

[3] Smart Networks and Services Joint undertaking (SNS-JU), https://smart-networks.europa.eu/

[4] European Partnerships to accelerate the green and digital transition, https://ec.europa.eu/info/news/commission-welcomes-approval-10-european-partnerships-accelerate-green-and-digital-transition-2021-nov-19_en

[5] Connecting Europe Facility (CEF), https://digital-strategy.ec.europa.eu/en/news/europe-sets-5g-investment-agenda-connected-and-automated-mobility

[6] Recovery and Resilience Facility instrument, https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en

[7] Digital Europe Programme (DEP), http s://digital-strategy.ec.europa.eu/en/activities/digital-programme

[8] EU 5G Cybersecurity Toolbox, Available at: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

[9] EU Cybersecurity Strategy, Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[10] European industrial strategy, Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_en

[11] SNS-JU Strategic Research and Innovation Agenda (SRIA), Available at: https://smart-networks.europa.eu/wp-content/uploads/2022/10/122021_sns_gb_decision_sria_including_annexdocx_89dnouztkolqi0m6dij7feh9da_82079_compressed-1.pdf

[12] 5G Strategic Deployment Agenda for Connected and Automated Mobility in Europe, Available at: https://5g-ppp.eu/wp-content/uploads/2020/10/20201002_5G_SDA_for_CAM_Final.pdf

[13] SNS R&I Work Programmes, Available at: https://smart-networks.europa.eu/reference-documents/

[14] United Nations Sustainable Development Goals (SDG), Available at: https://sdgs.un.org/goals

[15] European Parliamentary Research Service (EPRS), Study on "Key enabling technologies for Europe's technological sovereignty", 2021, Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697184/EPRS_STU(2021)697184_EN.pdf

[16] Horizon 2020 COREnect project, https://www.corenect.eu/

[17] Final COREnect Industry Roadmap. Deliverable D3.6, June 2022, Available at: COREnect_D3.6_Final_COREnect_Industry_Roadmap.pdf (squarespace.com), https://static1.squarespace.com/static/5f46601a7f9764175fb38f1c/t/62cfd87c20a77659f3b029a

0/1657788588357/COREnect_D3.6_Final_COREnect_Industry_Roadmap.pdf.

[18] Core Technologies Development Recommendations and Guidelines. Deliverable D3.7, June 2022, Available at: COREnect_D3.7_Core+Technologies+Development+Recommendations+and+Guidelines.pdf (squarespace.com), https://static1.squarespace.com/static/5f46601a7f9764175fb38f1c/t/6294ab1b5405c476fbdf31ad/1653910300850/COREnect_D3.7_Core+Technologies+Development+Recommendations+and+Guidelines.pdf.

[19] COREnext: European Core technologies for the next generation Communication-Computing hardware, https://corenext.eu

[20] Blog Pots by Thierry Breton, 20 December 2021, IPCEI on microelectronics – A major step for a more resilient EU chips supply chain available at: https://ec.europa.eu/commission/commissioners/2019-2024/breton/blog/ipcei-microelectronics-major-step-more-resilient-eu-chips-supply-chain_en.

[21] Smart Networks and Services Joint Undertaking: SNS R&I Work Programme 2021-2022. Available at: https://smart-networks.europa.eu/wp-content/uploads/2022/10/snsriworkprogramme20212022_ckvqrabs7gkb08dhgl6wh73cwqa_82061-6.pdf

[22] Smart Networks and Services Joint Undertaking: SNS R&I Work Programme 2023-2024. Available at: https://smart-networks.europa.eu/wp-content/uploads/2022/12/sns_ri_wp_2023-24.pdf

[23] NetworldEurope, Strategic Research and Innovation Agenda 2022, Available at: https://bscw.5g-ppp.eu/pub/bscw.cgi/d516608/SRIA-2022-WP-Published.pdf

[24] NetworldEurope, Strategic Research and Innovation Agenda 2022, technical Annex, available at: https://bscw.5g-ppp.eu/pub/bscw.cgi/d516614/SRIA%202022%20Technical%20Annex%20Published.pdf

[25] About Gaia-X - Gaia-X: A Federated Secure Data Infrastructure, Available at : https://gaia-x.eu/what-is-gaia-x/about-gaia-x/

[26] Manifesto for the development of the next generation cloud infrastructure services capabilities in 2022, Available at : https://www.bmwk.de/Redaktion/EN/Downloads/M-O/manifesto-for-the-development-of-the-next-generation-cloud-infrastructure-services-capabilities-in-2022.pdf?__blob=publicationFile&v=2

[27] The European High Performance Computing Joint Undertaking, available at: https://digital-strategy.ec.europa.eu/en/policies/high-performance-computing-joint-undertaking

[28] Sylva Project, Operators Telco Cloud white paper, available at: https://gitlab.com/sylva-projects/sylva/-/blob/main/White_Paper_Operators_Sylva.pdf

[29] The Linux Foundation Europe Launches to Foster European Open Source Collaboration and Innovation https://linuxfoundation.eu/newsroom/lf-europe-launches?hsLang=en

[30] Sylva project FAQ, https://gitlab.com/sylva-projects/sylva/-/blob/main/FAQ_Sylva.pdf

[31] M. Latva-aho and K. Leppänen. (eds.). "Key drivers and research challenges for 6G ubiquitous wireless intelligence," White paper, 6G research visions, No. 1. University of Oulu, Finland, 2019, Available at: http://jultika.oulu.fi/files/isbn9789526223544.pdf

[32] M. A. Uusitalo et al., "6G vision, value, use cases and technologies from European 6G flagship project Hexa-X," IEEE Access, vol. 9, pp. 160004-160020, 2021, Available at:

https://ieeexplore.ieee.org/document/9625032

[33] 6G-IA, European Vision for the 6G Network Ecosystem, Version 1.0, DOI: 10.5281/zenodo.5007671, June 2021, Available at: https://5g-ppp.eu/wp-content/uploads/2021/06/WhitePaper-6G-Europe.pdf

[34] 5G PPP Technology Board, AI and ML- Enablers for Beyond 5G Networks, Version 1.0, DOI 10.5281/zenodo.4299895, Available at: http://doi.org/10.5281/zenodo.4299895

[35] Universal Declaration of Human Rights, Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights

[36] Network and INformation Systems, NIS 2 DIrective, Available at; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557&qid=1677478161807

[37] Regulation, Cyber Act, Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1677478330880

[38] Proposal for regulation, Cyber Resilience Act, Available at: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[39] CYber Security Strategy, Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[40] Proposed regulation, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

[41] ENISA threat landscape for 5G Networks, Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

[42] The EU toolbox for 5G security, Available at: https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

[43] TNO 2022 R10507, Bridging the Dutch and European Digital Sovereignty gap, Available at https://www.tno.nl/en/importance-digital-sovereignty/.

[44] New DESI 2022: EU countries still struggle to close gaps in digital skills, Available at https://digital-skills-jobs.europa.eu/en/latest/news/new-desi-2022-eu-countries-still-struggle-close-gaps-digital-skills

[45] Commission kick-starts work on the European Year of skills, Available at: https://ec.europa.eu/social/main.jsp?langId=en&catId=1146&furtherNews=yes&newsId=10431

[46] Report of the World Commission on Environment and Development: Our Common Future, Available at: http://www.un-documents.net/our-common-future.pdf

[47] United Nations – Sustainability, Available at: https://www.un.org/en/academic-impact/sustainability

[48] United Nations - Social Development for Sustainable Development, Available at: https://www.un.org/development/desa/dspd/2030agenda-sdgs.html

[49] EC, The European Green Deal, Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:b828d165-1c22-11ea-8c1f-01aa75ed71a1.0002.02/DOC_1&format=PDF

[50] A European Green Deal - Striving to be the first climate-neutral, Available at: continenthttps://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en

[51] HEXA-X project, https://hexa-x.eu/

[52] Hexa-X Project, Deliverable D1.2, Expanded 6G Vision, use cases and societal values, Available at : https://hexa-x.eu/wp-content/uploads/2022/04/Hexa-X_D1.2_Edited.pdf

[53] AIOTI, "AIOTI IoT and Edge Computing Carbon Footprint Measurement Methodology, R1.1",, November 2022, Available at: https://aioti.eu/wp-content/uploads/2022/11/AIOTI-Carbon-Footprint-Methodology-Report-Final-R1.1.pdf

[54] Demassieux, N., 6G. Why?, European Conference on Networks and Communications, 2020, Available at: https://www.eucnc.eu/wp-content/uploads/2020/07/2020-05-29-6G.-Why-Nicolas-Demassieux-EUCNC-VDEF.pdf

[55] D-T. Phan-Huy, D. Barthel, P. Ratajczak, R. Fara, M. Di Renzo and J. de Rosny, "Ambient Backscatter Communications in Mobile Networks: Crowd-Detectable Zero-Energy-Devices," IEEE International Conference on RFID Technology and Applications (RFID-TA), 2021, Available at: https://ieeexplore.ieee.org/document/9617328

[56] V. Messié, B. Radier, V. Q. Rodriguez, G. Fromentoux, S. Vaton and I. Amigo, "A decentralised data layer for collaborative End-to-End service assurance," 2022 25TH CONFERENCE ON INNOVATION IN CLOUDS, INTERNET AND NETWORKS (ICIN), Paris, France, 2022, pp. 81-85, doi: 10.1109/ICIN53892.2022.9758094, Available at: https://ieeexplore.ieee.org/document/9758094

[57] The Mobile Economy Europe, GSMA, Available at: https://www.gsma.com/mobileeconomy/europe/

[58] ETNO, State of digital communications 2023, Available at: https://etno.eu/library/reports/112-the-state-of-digital-communications-2023.html

[59] AXON Partners Group, Europe's internet ecosystem: socio-economic benefits of a fairer balance between tech giants and telecom operators, May 2022.

[60] Identifying Europe's recovery needs, European Commission, Available at: : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0098&from=EN

[61] Gigabit Infrastructure Act Proposal and Impact Assessment, European Commission, Available at: https://digital-strategy.ec.europa.eu/en/library/gigabit-infrastructure-act-proposal-and-impact-assessment

[62] EU Commission launches Connectivity Package with 'fair share' consultation, Available at: https://www.euractiv.com/section/digital/news/eu-commission-launches-connectivity-package-with-fair-share-consultation/

[63] What societal values will 6G address? Societal Key Values and Key Value Indicators analysed through 6G use cases, 6G-IA White paper, Available at: https://5g-ppp.eu/wp-content/uploads/2022/05/What-societal-values-will-6G-address-White-Paper-v1.0-final.pdf

ABBREVIATIONS AND ACRONYMS

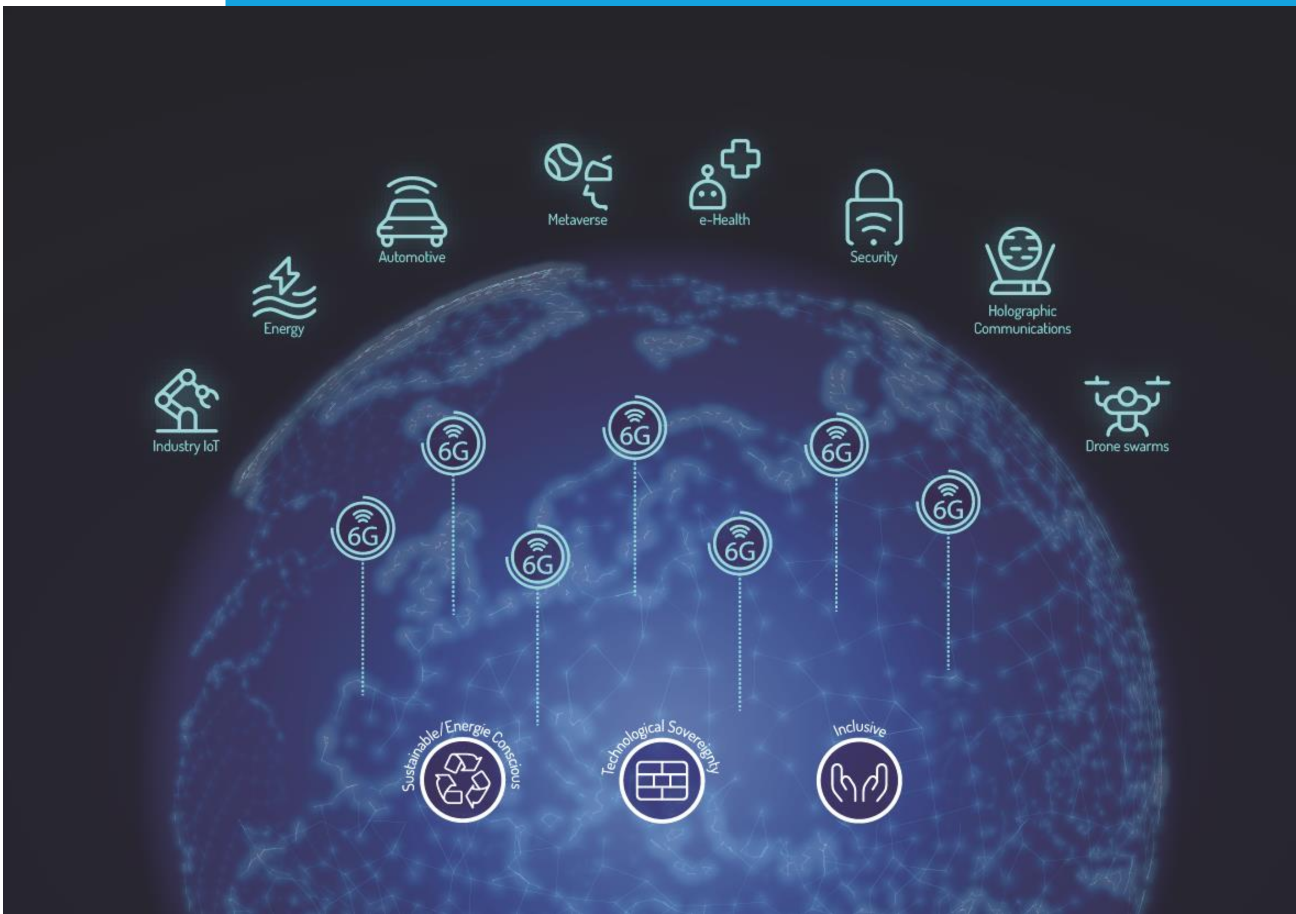
Acronym	Explanation
5GPPP	5G Public Private Partnership
6G-IA	6G Smart Networks and Services Industry Association
AI/ML	Artificial Intelligence – Machine Learning
AIOTI	Alliance for Internet of Things Innovation
API	Application Programming Interfaces
CAPEX	Capital Expenditure
CERT	Computer Emergency response Team
CO2	Carbon Dioxide
COTS	Commercial-off-the-shelf
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
DEP	Digital Europe Programme
DU	Distributed Unit
EC	European Commission
EMF	Electro-magnetic force
EMS	Electronic Management System
ETP	European Technology Platform
EU	European Union
FAQ	Frequently Asked Questions
GDP	Gross domestic product
GDPR	General Data Protection Regulation
HEU	Horizon Europe Framework
HPC	High Performance Computing
HW	Hardware
ICT	Information and Communication Technology
IoT	Internet of Things
IPCEI	Important Project on Common European Interest
JU	Joint Undertaking
KDT	Key Digital Technologies
KET	Key Enabling Technologies
KPI	Key Performance Indicators
KV	Key Value
KVI	Key Value Indicators
MNO	Mobile Network Operators
MSSP	Managed Security Service Provider
OPEX	Operational Expenditure
rApps	Non-real-time application
R&D	Research & Development
R&I	Research and Innovation
RAN	Radio Access Network

RU	Radio Unit
SDG	Sustainable Development Goals
SNS	Smart Networks and Services
SOC	Security Operating Centre
SRIA	Strategic Research and Innovation Agenda
SW	Software
SWOT	Strengths, weaknesses, opportunities, and threats
TBT	Technical Barriers to Trade Agreement
TCO	Total Cost of Ownership
TRL	Technology Readiness Level
VR	Virtual Reality
WTO	World Trade Organization
xApps	Near real time applications
xDR	Extended Detection and Response

LIST OF EDITORS AND CONTRIBUTORS

Surname	***Name***	***Editor/Contributor***	***Company / Institute / University***
Anton Haro	Carles	Contributor	CTTC
Bourse	Didier	Contributor	NOKIA
Ciulli	Nicola	Contributor	Nextworks
De Peppe	Raffaele	Contributor	TIM
Dotaro	Emmanuel	Contributor	Thales
Filipovic	Damir	Contributor	AIOTI
Garcia	Altor	Contributor	Vodafone
Kaloxylos	Alexandros	Editor/contributor	6G-IA
Lerquin	Christine	Contributor	RHEA
Lønsethagen	Håkon	Contributor	Telenor
Mohr	Werner	Editor/contributor	6G-IA
Norp	Toon	Contributor	TNO
Osseiran	Afif	Contributor	Ericsson
Quintuna Rodriguez	Veronica	Contributor	Orange
Schubert	Martin	Contributor	Huawei Munich Research Center (MRC)
Schulz	Egon	Contributor	Huawei Munich Research Center (MRC)
Trichias	Konstantinos	Contributor	6G-IA
Wikström	Gustav	Contributor	Ericsson
Willcock	Colin	Contributor	NOKIA

6G-IA is the voice of European Industry and Reseach for Next Generation Networks and Services



Contact: Office@6g-ia.eu

Website: https://6g-ia.eu/

DOI: 10.5281/zenodo.8315347

URL: https://6g-ia.eu/plans-papers/