EUROPEAN INDUSTRY WHITE PAPER ON
THE EUROPEAN QUANTUM COMMUNICATION INFRASTRUCTURE

Artist's view of a European Quantum Communication Infrastructure

Contents

Thales – Airbus – Opton Lasers – QTLabs – InfiniQuant – Fraunhofer – LusoSpace - Telefónica – KPN – GMV – Single Quantum – Toptica – Veriqloud – AIT – LuxTrust – Sitael – Eutelsat – IT4Innovation – Leonardo – OHB – SES – Telsy – QuSide – Ariane Group

EXECUTIVE SUMMARY

The European industry strongly supports the development of a Quantum Communication Infrastructure (QCI) that would in a first stage secure government and critical infrastructure communication across the European Union, and in a second stage prepare the connection of quantum computers and sensors in a full Quantum Information Network. This support is motivated by the following considerations.

- The QCI will provide an unprecedented way of securing communications among structuring entities of the European society, to guarantee its continued development in an increasingly troubled international environment. It adds physical security to the current algorithm security.
- The QCI will contribute to developing the new ecosystem of quantum technologies, which will be key for the strategic autonomy of our Union, both for security-related aspects as well as regarding leadership on the global market of high-performance devices based on quantum technologies. It will also create and maintain highly skilled jobs in Europe, thus contributing to the long-term economy and welfare for the European society.
- The QCI programme will be the tool through which the public sector will take its stake in the needed high-risk investment that will help the European quantum communications ecosystem emerge for the shared benefits of the whole Union, and allow subsequent commercial uses.
- The QCI will be the first step towards a completely new information exchange through Quantum Information Networks, which will enhance the performance of processors and sensors, and will allow creating in the long term a wide range of commercial applications.

The European industry players recommend the following actions that would permit to step forward in the development and deployment of the QCI.

- Define in the coming months the stage 1 (2021-2028, *Quantum-Secured Networks*) and stage 2 (2028-2035, *Quantum Information Networks*), and gather funding at the European Commission.
- Define in the coming months the structuring *user requirements* and derive them on the *terrestrial and space components* of the overall architecture.
- Start the *development of European terrestrial products* to be progressively integrated in metropolis-scale networks early in the upcoming Multiannual Financial Framework (MFF).
- Start the space segment trade-off/architecture studies for a development and technology plan definition including necessary in-orbit demonstration as early as possible in the upcoming MFF.
- In the second half of the upcoming MFF, complete the deployment of the terrestrial local networks and develop the operational elements of the space component and of the resulting hybrid network management and operation means by 2028.
- In parallel, launch the preparation of the technology transfer from laboratory to industry for the terrestrial and space equipment needed to reach the second objective of the QCI – building a complete Quantum Information Network along the next MFF (2028-2034).
- In parallel, universities shall be incentivised to educate quantum engineers, a topic of utmost importance for a successful QCI ecosystem.
- In parallel, European law makers should generate the needed legislation in order to regulate the aspects of QCI rights, use and competition, and support industry in the creation of appropriate international standards.

The Industry considers that the QCI has strong similarities with Galileo and that its development and deployment could be organised similarly in many aspects.

WHY DOES EUROPE NEED TO ACT NOW?

Quantum communication breakthroughs

Quantum communication technologies leverage the transfer of quantum information from one place to another. These technologies range from exploiting the inherent randomness of quantum measurements to produce high quality cryptographic keys to share secrets (quantum cryptography, quantum money, quantum auctions, quantum vote, quantum commitment…) to transferring complete quantum information e.g. from one quantum processor to another, using quantum state teleportation. One of the main features of Quantum Communications is that any eavesdropping on a communication line is detectable by the laws of quantum physics. This means that an entity that masters this technology is able to communicate in a controlled concealed way from any other actor. Beyond this, the sub-field of quantum cryptography (a.k.a. *Quantum Key Distribution*, QKD, with many different protocols) allows an inherently safe way to establish encryption keys among actors, without relying on complex mathematical problems that quantum computers will probably solve in the coming years, thus cracking the codes. It further does not require complex manned key distribution procedures that involve agents that can betray, and material that can be copied, even though it does require a very good physical layer implementation. In other words, quantum cryptography allows a new way to secure communication against eavesdropping/wire-tapping, in a way that is advantageous with respect to current solutions and is future-proof for data storage.

Social and political interest.

Our world is undergoing a profound redistribution of the centres of powers, and this leads a number of unidentified actors to opportunistically take their chance, in one-shot operations or in longer term political influence operations. These operations are rarely violent, and often occur in cyberspace. To give just two recent examples, this can be through the use of ransomware to block a national health system, or through theft of confidential information to reveal it to the public to influence elections. To be robust in this moving environment, Europe needs to develop all elements that will enable the continued protection of its critical infrastructure and interests with an adequate level of secrecy and security. Quantum technologies are no strangers in this. On the one hand, quantum computers are likely to disrupt the asymmetric key encryption protocols commonly used in security solutions today. On the other hand, quantum communications show new ways of communicating, that are protected from these disruptions. If an entity has this technology and Europe has not, the result is a position of clear inferiority in terms of communications sovereignty.

Developing a first quantum communication infrastructure will create a momentum that will foster progress on the quantum communication technologies, and will allow preparing the next step, that will be full *Quantum Information Networks* (QIN) to connect e.g. quantum processing farms.

Due to the completely new opportunities that quantum technologies bring to fields of activities that have already shown vast interest in our economies (communication, computation, etc.), *quantum technologies are in a position to become one of the core technical engines of the next step of our society development*. It is thus key for an ambitious Europe that wants to be at the forefront of global development to invest in what are likely to be the foundations of this development.

This is particularly true in the case of quantum-enhanced secure communications, where many countries are currently ahead of Europe.

- China has expanded a European-inherited know-how to an unprecedented level, by deploying a more than 2000km terrestrial network from Shanghai to Peking that is protected by quantum cryptography, and by demonstrating longer range possibilities using satellites (Micius mission), for both cryptography and

teleportation. Asian-owned companies already have commercial terrestrial products, and have experimented satellite components in space.

- The USA have been pioneering these technologies since the beginning of this century, by deploying the first networks at the Los Alamos National Laboratory, as well as in the Boston area back in 2002. Now, there is an emerging industrial ecosystem in the USA East Coast. It is very likely that public information on this topic has been limited, keeping most of it for American eyes only.
- Within European-owned companies, there is a very good industrial know-how on the fundamentals (quantum communications and ancillary fields like fibre networks, optical communications, satellite systems,) as well as on large scale tests of terrestrial equipment. These assets and know-how need now be developed into a fully operational large scale system that could address societal and strategic needs of Europe. Regarding the space component of such a large scale system, the needed know-how is available and several companies already have roadmaps to develop equipment and systems for it.
- Although the strategic needs for Europe are clear and self-evident, commercial applications are lagging behind due to a wealth of interconnected issues. To reap the full benefit of quantum-enhanced secure communication, one would need the above mentioned large scale system already existing, a number of users already subscribed to it, available end-user terminals and a clear set of inter-operability standards for use in mainland Europe and beyond. In such a perspective, our companies are scanning for potential markets to motivate our stockholders to invest in the next step, from R&D phase, up to a product & service phase. The QCI, on top of being the solution of choice for EU institutions, could also trigger the start of commercial applications driven by the private sector at some point in time, for example by feeding the market with the first public anchor customers, or planning a shared use of the QCI between public and private users.
- The European Union can bring this market into existence by a) creating an ambitious infrastructure programme b) creating awareness in the public on the importance of cyber security and the role of QKD; c) creating the needed legislation to define the rules for such market; d) pursuing R&D effort on quantum security while initiating R&T to prepare the next steps. There is already a positive experience to inspire us. Mobile communication technologies as we know them now have been invented in Europe, along with the infrastructure and the market rules, and then have expanded beyond Europe to the rest of the world.

The European Union must scale up the effort to keep up with the global pace of developments in this field, a field that industry considers as strategic for the Union's digital autonomy and sovereignty.

OBJECTIVES FOR AN AMBITIOUS EUROPEAN PROGRAMME AND THEIR MOTIVATIONS

Motivation

A communication network puts by definition users in contact, and the more the users the higher the added value the network brings. This also applies to a quantum communication networks.

However, the costs of creating a large-scale quantum network might prove daunting to private investors. On the one hand, limiting the risk by limiting the first investments might jeopardise the achievement of a self-sustainable minimum viable product. On the other hand, the investment required to set up a quantum communication network large enough to be self-sustaining is too high for the current perception of the market. In such a case, a public infrastructure is the right answer to kick-start both market and investments.

The experience of the development of telecommunication networks in the past century shows that many unexpected and sophisticated uses of communication can emerge from an infrastructure that has been developed for a more basic purpose ('talking at a distance'). This will also be the case of Quantum Communications. Yet, the

step from basic use to an advanced use that could attract private investors is way too risky to expect a sufficient investment of private actors on this first step.
Both these motivations explain why the European public bodies need to seize this topic and bootstrap the domain through an ambitious programme for a quantum communication infrastructure.

There are several, staggered objectives that can be setup for this ambitious programme, taking into account the inherent limitations and different levels of maturity of the various uses that can be made of quantum technologies.

Maturity

The most mature applications today exploit only a part of the quantum communication capabilities. *Quantum cryptography* is the most advanced one. A large number of protocols have been devised in this sub-field, a good number of which are mature both from the perspectives of security and of the material implementation in terrestrial networks. There are commercial products available on the market, and the next step that needs be taken is the establishment of adequate security standards. That would allow a third-party certification to consolidate the level of trust in these systems from an external user point of view. This can be made operational on ground in the short term.

Even more promising is the exploitation of the full transfer of quantum information in *Quantum Information Networks* (QIN) – enabling the pooling of quantum computers by allowing them to directly exchange quantum information with one other, hence increasing the computational power of the whole. This will allow expanding the computational power even faster than the equivalent networking of classical computers. Networks of quantum sensors that would exchange the q-bits resulting from their measurements are also likely to increase by orders of magnitude their performance. Products for this kind of applications are still to be developed, based on devices operated daily in laboratories for the past 20 years. With the support of institutional R&T budget, this needs first to be matured by industry and scientific laboratories and then to be made operational in the 2030's.

Limitations

The main limitation of quantum communications results from the combination of two main elements. First the quantum signals are by essence much weaker than the classical communications, but are subject to the same level of fading in their propagation. Second, it is impossible to copy a quantum state without destroying a part of the information it contains. Even though this allows confidentiality, and is thus a point of strength of quantum communication, it means that the classical concept of repeater is not applicable anymore. Quantum signals are usually visible-light or near-infrared signals, transmitted by lasers in optical fibres reminiscent from optical telecommunication technologies. For this reason, terrestrial quantum communication use fibre-optics networks to implement quantum communication. This means a strong limitation of terrestrial networks, as optical fibre absorbs 0,2dB/km, after a few tens kilometres in terrestrial networks, there is no signal left and the quantum communication stops.

In free-space communication, it is possible to shine a laser in open space, and obtain a much lower level of losses than in fibre and therefore an increased range to reach thousands of kilometres. This is where satellites have a natural role to play in quantum communication infrastructures. Satellite overcome the distance limitations that would be otherwise impossible, impractical or uneconomical to cover by ground networks . On top of this, a satellite is an asset which is costly to attack as compared to ground nodes.

Proposed objectives for the QCI implementation programme

The Industry recommends thus to structure the European programme to develop a Quantum Communication Infrastructure (QCI) by the following simple objectives.

- First, develop and deploy an infrastructure to support quantum-enhanced secure communications at continent scale by 2028. This will allow securing public communication between government offices as well as within infrastructures that are vital for Europe (electricity grids, air traffic control, hospitals, etc.) in European countries and beyond where needed (e.g. embassies, critical European interests, interfaces with allied countries, etc.). This very infrastructure could be operated for Europe by a commercial operator, or be shared with commercial applications in other ways, so as to kick-start the private market in this field.
- Second, expand this infrastructure to make it more capillary, and expand the uses of this infrastructure to support complete quantum information networks by 2035
- The objective of 2028 will require deploying both a terrestrial and a space component. Since the terrestrial elements are more advanced, the development of the space component shall be a priority due to the longer lead time required, although European sources of terrestrial operational material should be expanded.
- The objective of QIN for 2035 will require the development of both terrestrial and space operational components. A part of the 2028 programme should be dedicated to initiate these longer term goals through dedicated R&T studies and developments, without jeopardising the secure communications priority.
- In parallel, European law makers should generate the needed legislation in order to regulate the aspects of rights, use and competition.

PRACTICAL CONSIDERATIONS

Users

The first users of the infrastructure could be government, or close-to-government entities. There are three reasons for this. The first one is that commercial market is not yet ready – awareness among potential customers is still limited – the investment required for a commercial market are too high and not well defined, and the associated market risk is perceived as "high". The second is that the high-end protection provided by this infrastructure will be most relevant for secure government communication as well as for the control layer of critical public infrastructure (power grid, air traffic control, health systems, data centres and High Power Computing centres, etc.). The third reason is that once encryption keys are provided by quantum cryptography, they can be used to protect stored data in a way that is future-proof since these keys have a controlled level of confidentiality and do not need to travel beyond the points where they are used, so minimise the risk of interception. And governments are the entities that have the longest secrecy requirements.

Use cases and user requirements

The first input that shall trigger the development and deployment of such an infrastructure is the definition of reference use cases and scenarios. Each scenario shall describe the uses that will be made of the infrastructure, and especially the requirements that the users have on the infrastructure in terms of types of service, interfaces and performance. There can be several use cases depending on the considered user category. and the pre-existing or complementary security solutions. It is important to understand for each scenario the role model (who makes what in the whole value chain), how the quantum infrastructure is integrated within global security solutions (e.g. secure cloud storage, password management, access control), the level of “trust” required and the associated (often hidden) costs.

A system

The QCI shall be considered as a single operational system. This system comprises a terrestrial component and a space component, with their necessary management and operation facilities. This system is developed and deployed to meet the needs of the users described in user requirements above. The organisation of the development work shall be such that once the user requirements are identified, the overall design of the components of the infrastructure shall be carried out in a coordinated way. All available quantum communication technologies will be considered for application in one or more components of the system in order to find optimal solutions. The governance and the operation model of the QCI shall be defined as early as possible in the process. It should also take into account service layer elements in support of a capillary adoption of Quantum communication based services across Europe. From a programme point of view, a combination of start-ups, SMEs and large enterprises is the key to success.

Start satellite early

The space component of the QCI will comprise one or several satellites using the most appropriate quantum communication protocol at orbits to be optimised. Space infrastructures usually need a very thorough development and test campaign, and need to be deployed minimising the launch cost. In the case of the space component of the QCI, technology maturation, started by some actors, will need be completed. This all adds up to make space infrastructure work inherently long. To target the date of 2028, it is key to start working on the space infrastructure as soon as possible with relevant trade-offs and architecture study. A technology and development plan will identify the activity to be fulfilled within the next MFF including necessary in-orbit demonstration by 2025 prior to the space segment deployment.

Define the security verification policy

A secure communication system needs to be developed and tested according to processes that allow guaranteeing the required level of security in a way that is accepted by all parties, especially with respect to the notion of *trust*. This verification policy shall be defined at least along the development of the system to avoid costly rework. Two kinds of frameworks can be considered.

- A first way can be through the establishment of industrial security standards requirements, approved by recognised certification bodies, that list security constraints and test procedures that the system shall pass. This is adapted to services delivered to a large audience, where the service provider is a third party that the users shall trust.
- A second way can be to establish a Programme Security Instruction that is a political agreement internal to the system stakeholders on the security conditions and the way to verify them, in the spirit of the Galileo PSI. This is more adapted to a system that is used by its owners, so users do not need to trust a third party.

Given the goals of the QCI, Industry recommends the second solution, although the experience should be used in parallel to derive standards that will be part of a wider regulation framework (as mentioned above), enabling a wider commercial use of quantum technologies. Note that quantum communication will require developing e.g. new penetration test techniques by security agencies.

Prepare full Quantum Information Networks (QIN)

The second objective of the quantum communication infrastructure, to prepare a complete Quantum Information Network by 2035 (to connect e.g. quantum processing centres across the continent, or support entanglement-based further applications), requires a wider step in maturity. This step will benefit from the means deployed to reach the first objective, although these will not be sufficient. In the 2021-2027 period while operational components will be developed and produced to reach the first objective of securing communications, a simultaneous effort shall be fostered in the industry, with links with scientific laboratories, to assess the feasibility to transfer QIN technologies

from laboratories to industry in order to prepare the second objective. The full industrialisation and operational deployment of these components will then be carried out in the second phase, in the 2028-2034 period.

IMPACT ON THE EUROPEAN ECONOMY AND SOCIETY

Societal impact

Quantum communication is one part of the answer to the threat of quantum computers, expected to break the asymmetric encryption schemes widely used nowadays to protect the data exchanged over communication networks. Even though powerful enough quantum computers are not known yet to be available to make this threat effective today, recording of sensitive communication data is probably already on-going, and will be deciphered when those quantum computers are here. The threat is thus actual, now, for all information that is supposed to remain secret for a long time.

The first societal impact of being able to use a quantum communication infrastructure at continent scale (e.g. among capital cities, but also Hamburg-München, Lyon-Toulouse, Zaragoza-Lanzarote, Szczecin-Krakow, Milano-Napoli, etc.) will be the benefit of a higher level of security of the public bodies that govern the society. It is all the more important in a world of growing tensions where intelligence and interference in government communications, as well as hazards to critical infrastructures are a real threat.

The second societal impact is in the longer term, given that such developments could trigger major society evolutions, comparable to the advent of electronics and of global communication networks. As a matter of fact, when a QCI is able to support more quantum communication uses, acting as a QIN, it will become the ground for a flourishing development in many areas of society and economy, the variety of which might be limited only by human imagination. This will contribute to the overall benefit for the EU citizens, by creating highly skilled jobs in highly technological and added-value application fields.

It is thus of a high societal relevance, both in short and long term, to develop the capabilities of a long-range QCI, and thus to start the definition, development and deployment of both components of this future communication system.

Benefits for member states

The System under consideration is a system to deliver a service for government and critical infrastructure use. There are thus immediate benefits for the member states: improve the security of their communication, improve the security of their critical infrastructures.

Beyond this direct benefit, the QCI will be the first step of a longer term ‘general purpose’ Quantum Information Network, that will allow many more applications than secure communications through quantum cryptography. In this sense, the QCI could be the equivalent of what ARPANET was in the 1960-70’s, and that gave birth to the current Internet. This QCI shall thus be considered with all the economic significance that we see in the current Internet.

Socio-economic benefits

Having a secured communication infrastructure for government services and critical infrastructure and beyond this, developing industrial capability in quantum technologies will have a number of socio-economic benefits.

Security - Secured communication throughout the governance of the Union and the providers of basic, critical services will make them more robust. Such a robust framework for the European society makes it less prone to destabilisation by external competitors, which we see every day more active. Protected from such destabilisations,

the citizens and the economic forces will have the environment to develop initiatives that will in turn expand prosperity and social return to the general public.

Technology - Beyond the benefits of a stable, secured social framework, the technological steps that will be taken to build a QCI will build capacity for quantum technologies related to communication for European actors. These technologies are likely to be the basis of a new industrial revolution, comparable to what the advent of electronics allowed 50 years ago. In this case, these technologies would be the new engine of a significant economic growth, all the more profitable to Europe as many industries are involved in it, driving social progress in many ways.

Employment - The launch of the deployment of large scale quantum-technology-based operational systems in Europe such as the QCI, will drive the emergence of a new economic sector in Europe that will bring its contribution to the job market. When this sector has benefitted from such first projects, it will be ready to address more commercial markets in Europe, and will be able to compete with other global actors, and through export outside Europe.

In all cases, we see that having a QCI at the scale of the European Union will contribute in making Europe a stronger actor on the global scene, in a secured context favourable to innovation and investments. This is a key for Europe to remain at the forefront of the global leadership.

COMPANY ENDORSEMENT

This document is endorsed by the following actors, by order of reply.

Thales Group
Member state: France
Represented by : Dr. Marko Erman
Position: SVP, Chief Technical Officer

Signature

Airbus
Member state: Germany
Represented by : Grazia Vittadini
Position: Chief Technical Officer

Signature

Opton Laser International
Member state: France
Represented by : Jean-Claude Sanudo
Position: President & CEO

Signature

Quantum Technology Laboratories GmbH
Member state: Austria
Represented by : Sam Leopold Tschernitz
Position: Chief Executive Officer

Signature

InfiniQuant Startup project
Member state: Germany
Represented by : Imran Khan
Position: Project leader

Signature

Fraunhofer Institute for Applied Optics and Precision Engineering IOF
Member state: Germany
Represented by : Prof. Dr. Andreas Tünnermann
Position: Director

Signature

LusoSpace
Member state: Portugal
Represented by : Ivo Vieira
Position: CEO

LUSOSPACE - PROJ. ENG., LDA.
LISBOA - PORTUGAL
☎ +351 213974363
NIF/VAT: 506263851
A GERENCIA:

Signature

Telefónica
Member state: Spain
Represented by: Dr. Luis Ignacio Vicente del Olmo
Position: Head of Intellectual Property & Return on Innovation

Signature

KPN
Member state: The Netherlands
Represented by : Mr Joost Farwerck
Position: CEO

Signature

GMV AD
Member state: Spain
Represented by :Miguel Angel Molina
Position: GMV Space Deputy General Manager

Signature

Single Quantum
Member state: The Netherlands
Represented by : Dr. Sander Dorenbos
Position: CEO

Signature

TOPTICA Photonics AG and TOPTICA Projects GmbH
Member state: Germany
Represented by : Dr. Wilhelm Kaenders
Position: CTO

Signature

VeriQloud
Member state: France
Represented by : Marc Kaplan
Position: President

AIT Austrian Institute of Technology GmbH
Member state: Austria
Represented by : DI Helmut Leopold, PhD / DI Dr. Martin Stierle
Position: Head of Digital Safety & Security Center / Head of Competence Unit

Signature

LuxTrust
Member state: Luxembourg
Represented by : Pascal Rogiest
Position: Chief Executive Officer

Signature

SITAEL SpA
Member state: Italy
Represented by : Dr. Pierluigi Pirrelli
Position: Space Division Managing Director

Signature

EUTELSAT S.A.
Member state: France
Represented by : Yohann LEROY
Position: CTO & Deputy CEO

Signature

IT4Innovations | National Supercomputing Center
Member state: : Czech Republic
Represented by: Dr. Vit Vondrak
Position: Managing Director

16. 10. 2019

Signature

Leonardo
Member state: Italy
Represented by : DR. Roberto Cingolani
Position: Chief Technology & Innovation Officer

Signature

OHB System AG
Member state: Germany
Represented by : Guy Perez
Position: Chief Technical Officer

Signature

SES
Member state: Luxembourg
Represented by : Christophe De Hauwer
Position: Chief Strategy & Development Officer

Signature

Telsy S.p.A.
Member state: Italy
Represented by : Ing. Fabrizio Vacca
Position: Chief Technology Office

Signature

Quside Technologies S.L.
Member state: Spain
Represented by : Carlos Abellan
Position: Chief Executive Officer

Ariane Group SA
Member state: France
Represented by : Morena Bernardini
Position: VP Strategy

Signature