BCO
Network

BCO Network WEBseries 17
Design and tendering for a public quantum network

23 September 2025

Speakers:

Petra Scudo, Joint Research Center, European Commission

Eduard Falco, BCO Catalonia

Funded by
the European Union

BCO
Network

Register to
2025 BCO Network
Annual Conference *and networking dinner*

Brussels, Belgium

06 October, 2025

To register, please fill in the **survey**
The agenda is available on Futurium

Deadline: October 1st

Funded by
the European Union

BCO
Network

Register to
Sixth Meeting of the Public Authorities Group on 5G for Innovation in Smart Communities

Brussels, Belgium

06 October, 2025

To register, please fill in the survey

The agenda is available on Futurium

Deadline: October 1st

Funded by
the European Union

BCO
Network

Register to
CEF Digital Conference & EDC Awards

Brussels, Belgium

07 October, 2025

Please register on the official website

The agenda is available on Futurium

Deadline: September 25th

Funded by
the European Union

BCO
Network

Register to

2025 5G Community Conference

Brussels, Belgium

08 October, 2025

To register, please fill in the survey
The agenda is available on Futurium

Deadline: October 1st

Funded by
the European Union

BCO
Network

Register to
European Regions Week

Connected to stay-Investing in digital connectivity for Europe’s rural, remote and outermost regions

Brussels, Belgium

15 October, 2025

To register, please visit the official website
The agenda is available on Futurium

Deadline: September 30th

Funded by
the European Union

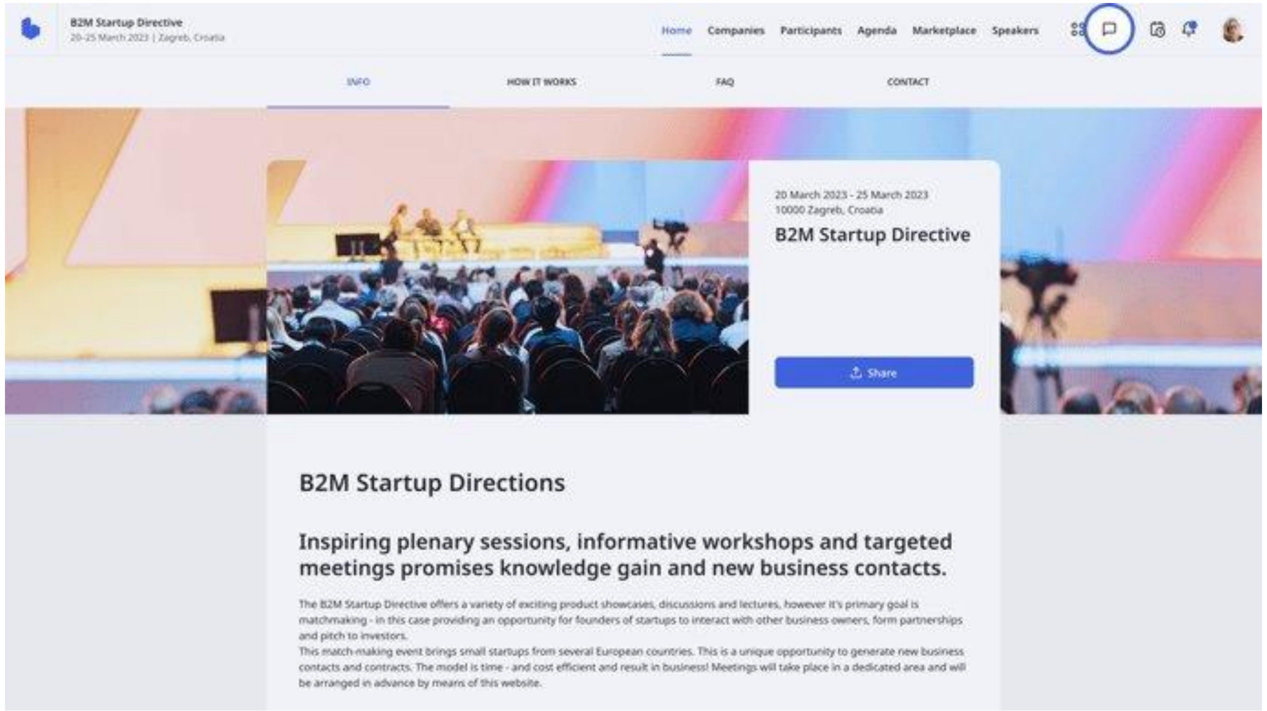
BCO
Network

The 5GSC Support Platform Features

To register, please create your profile here

BCO
Network

5GSC Support Platform: Conversations



B2M Startup Directive
20-25 March 2023 | Zagreb, Croatia

20 March 2023 - 25 March 2023
10000 Zagreb, Croatia
B2M Startup Directive

B2M Startup Directions

Inspiring plenary sessions, informative workshops and targeted meetings promises knowledge gain and new business contacts.

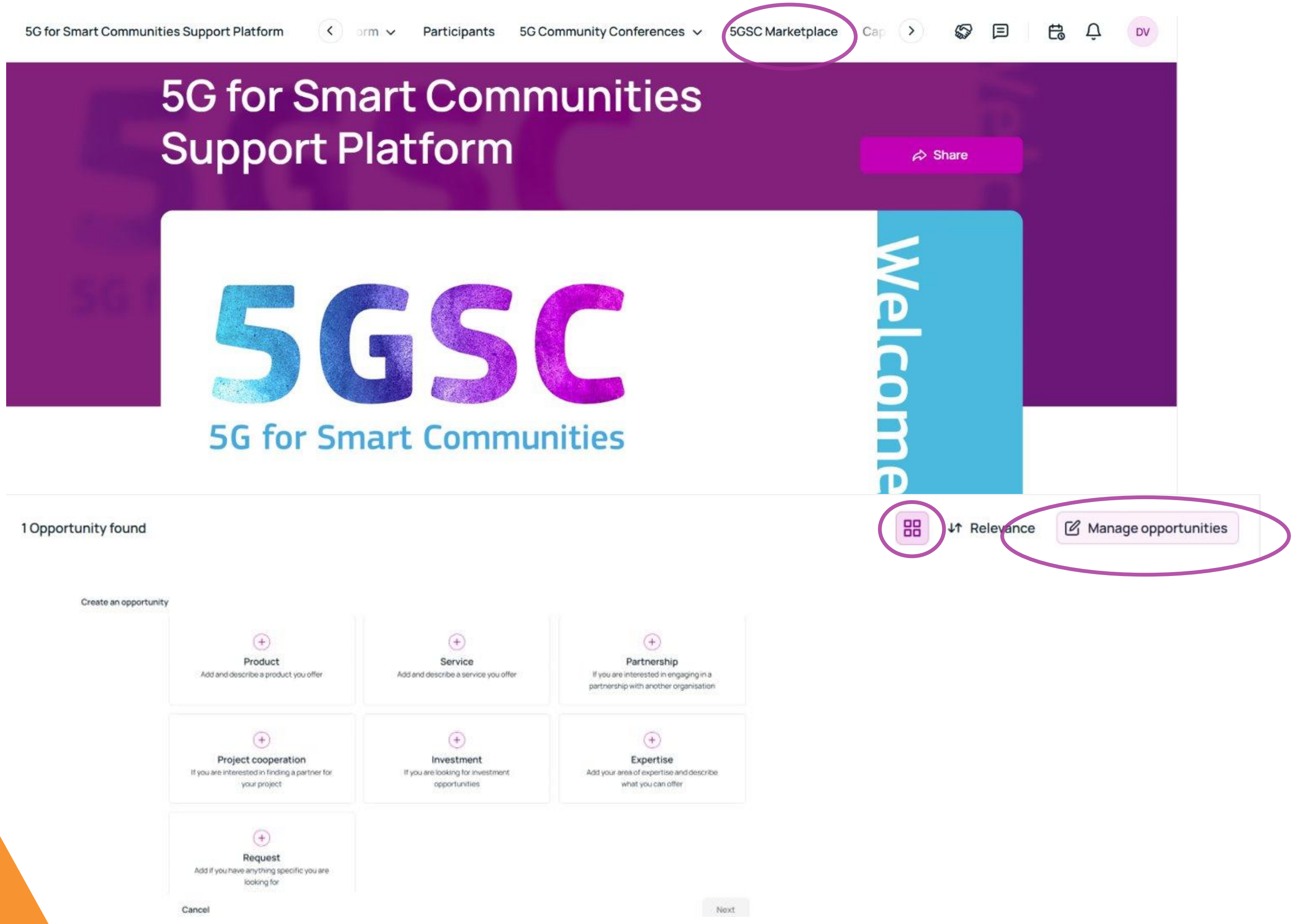
The B2M Startup Directive offers a variety of exciting product showcases, discussions and lectures, however it's primary goal is matchmaking - in this case providing an opportunity for founders of startups to interact with other business owners, form partnerships and pitch to investors.
This match-making event brings small startups from several European countries. This is a unique opportunity to generate new business contacts and contracts. The model is time - and cost efficient and result in business! Meetings will take place in a dedicated area and will be arranged in advance by means of this website.

Conversations

- ✓ Add up to 8 people
- ✓ Direct message participants
- ✓ By clicking the staple icon, attach images and documents to the chat
- ✓ All conversations are private

Funded by
the European Union

The 5GSC Platform: Marketplace



1 Opportunity found

Create an opportunity

- Product – Add and describe a product you offer
- Service – Add and describe a service you offer
- Partnership – If you are interested in engaging in a partnership with another organisation
- Project cooperation – If you are interested in finding a partner for your project
- Investment – If you are looking for investment opportunities
- Expertise – Add your area of expertise and describe what you can offer
- Request – Add if you have anything specific you are looking for

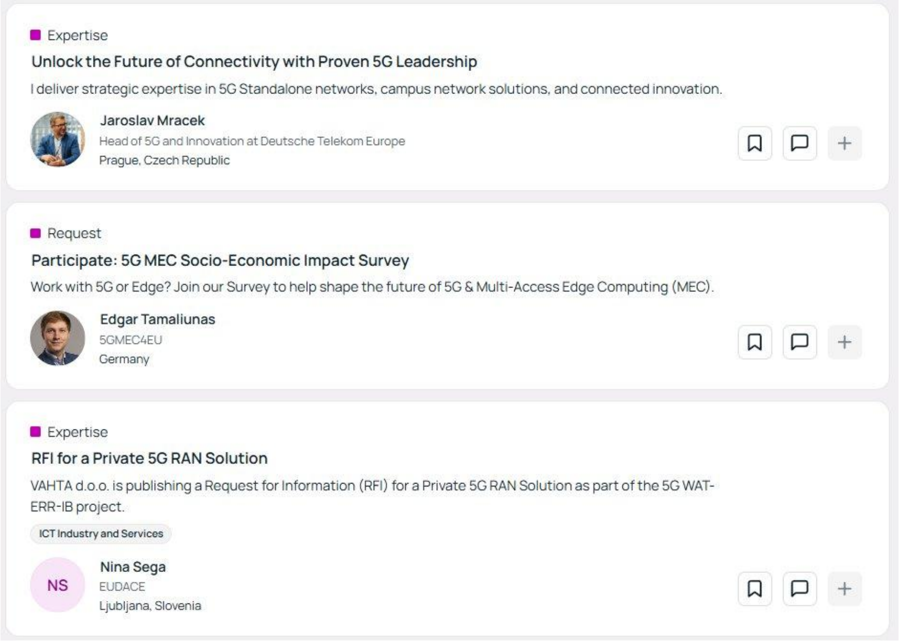
Marketplace

- ✓ Login to the platform
- ✓ Go to **5GSC Marketplace**
- ✓ Choose to view opportunities in a list or grid view or filter them by relevance or creation date
- ✓ Manage opportunities & create an opportunity – add images, files and videos

Funded by
the European Union

The 5GSC Platform: Marketplace

5GSC Marketplace



Expertise

Unlock the Future of Connectivity with Proven 5G Leadership

I deliver strategic expertise in 5G Standalone networks, campus network solutions, and connected innovation.

Jaroslav Mracek
Head of 5G and Innovation at Deutsche Telekom Europe
Prague, Czech Republic

Request

Participate: 5G MEC Socio-Economic Impact Survey

Work with 5G or Edge? Join our Survey to help shape the future of 5G & Multi-Access Edge Computing (MEC).

Edgar Tamaliunas
5GMEC4EU
Germany

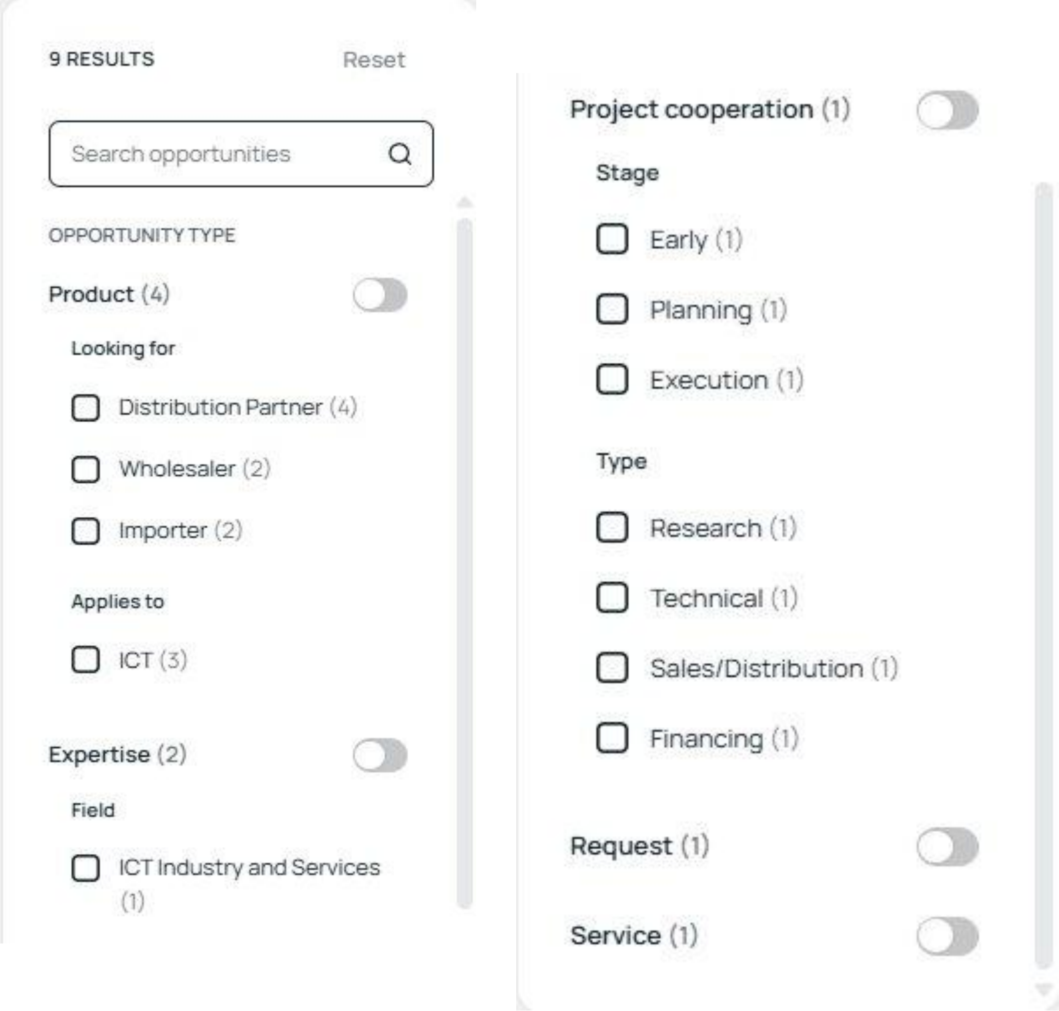
Expertise

RFI for a Private 5G RAN Solution

VAHTA d.o.o. is publishing a Request for Information (RFI) for a Private 5G RAN Solution as part of the 5G WAT-ERR-IB project.

ICT Industry and Services

NS Nina Sega
EUDACE
Ljubljana, Slovenia



9 RESULTS Reset

Search opportunities

OPPORTUNITY TYPE

Product (4)

Looking for

□ Distribution Partner (4)
□ Wholesaler (2)
□ Importer (2)

Applies to

□ ICT (3)

Expertise (2)

Field

□ ICT Industry and Services (1)

Project cooperation (1)

Stage

□ Early (1)
□ Planning (1)
□ Execution (1)

Type

□ Research (1)
□ Technical (1)
□ Sales/Distribution (1)
□ Financing (1)

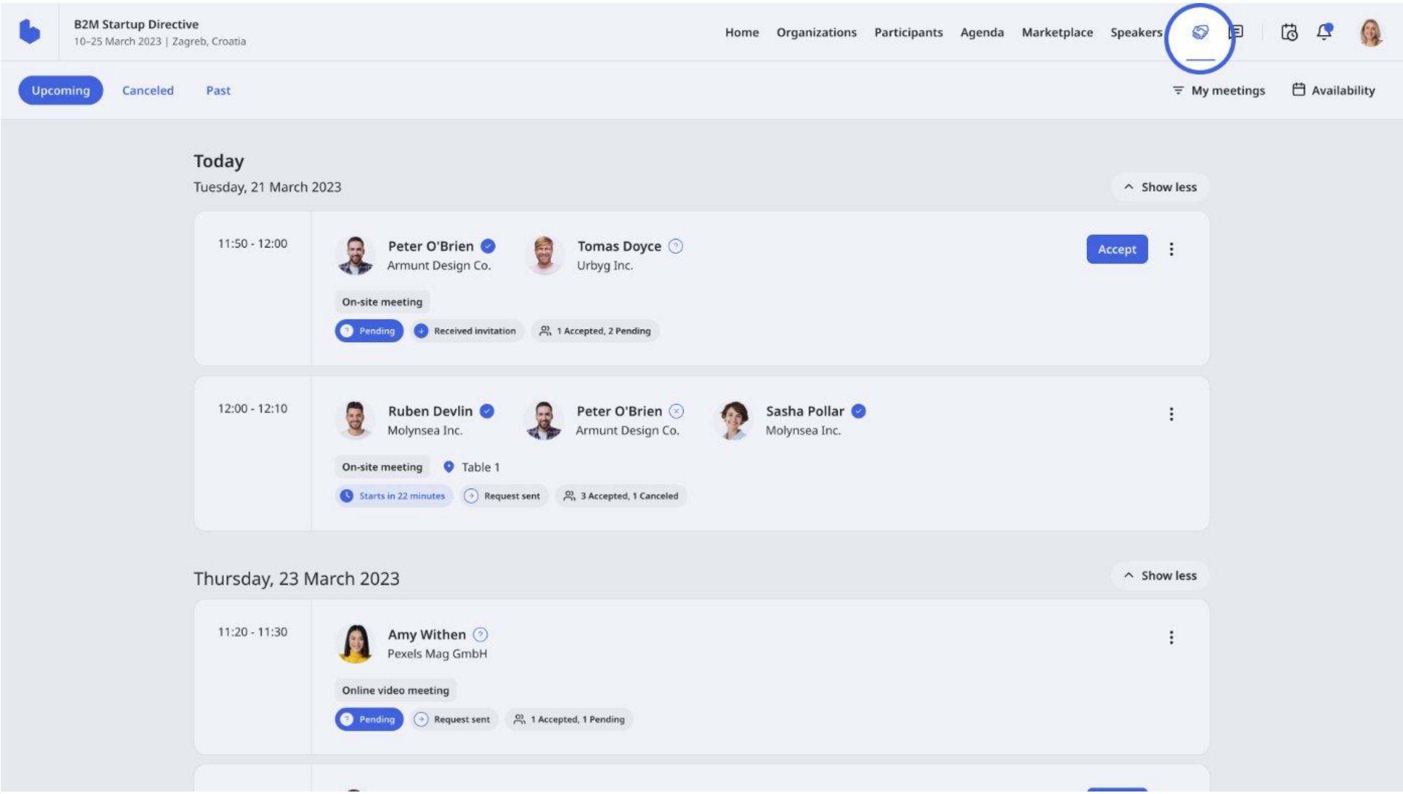
Request (1)

Service (1)

Funded by
the European Union

BCO
Network

The 5GSC Platform: Meetings



B2M Startup Directive
10–25 March 2023 | Zagreb, Croatia

Today
Tuesday, 21 March 2023

11:50 - 12:00
Peter O'Brien, Armunt Design Co.
Tomas Doyce, Urbyg Inc.
On-site meeting
Pending · Received invitation · 1 Accepted, 2 Pending

12:00 - 12:10
Ruben Devlin, Molynsea Inc.
Peter O'Brien, Armunt Design Co.
Sasha Pollar, Molynsea Inc.
On-site meeting · Table 1
Starts in 22 minutes · Request sent · 3 Accepted, 1 Canceled

Thursday, 23 March 2023

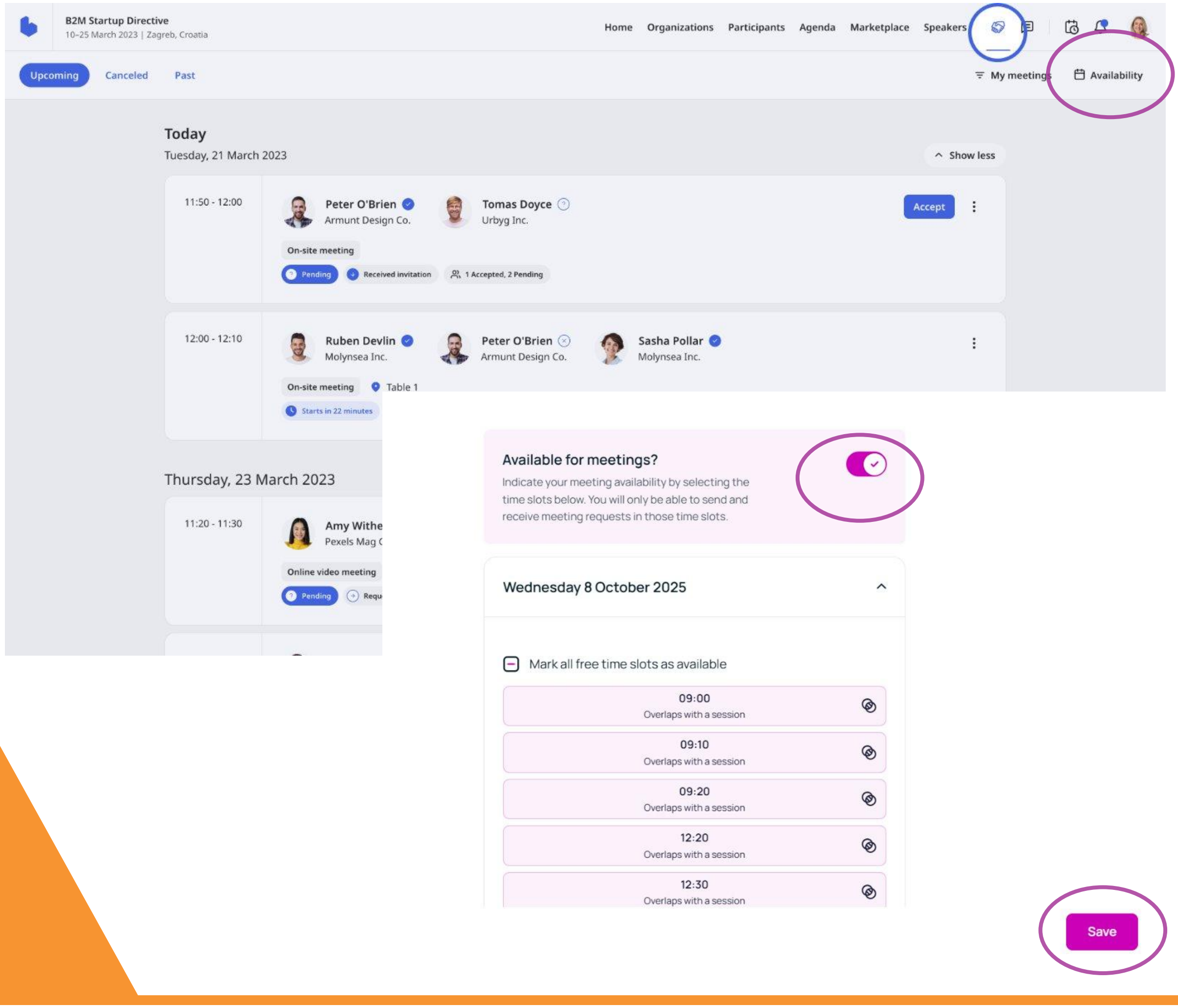
11:20 - 11:30
Amy Withen, Pexels Mag GmbH
Online video meeting
Pending · Request sent · 1 Accepted, 1 Pending

Meetings

- ✓ Up to 8 people
- ✓ **Online video meetings & onsite 5G Community Conference October**
- ✓ Check meeting status: upcoming, cancelled, past
- ✓ Request meetings

Funded by
the European Union

The 5GSC Platform: Meetings



Today
Tuesday, 21 March 2023

11:50 - 12:00 Peter O'Brien, Armunt Design Co. · Tomas Doyce, Urbyg Inc.
On-site meeting
Pending · Received invitation · 1 Accepted, 2 Pending

12:00 - 12:10 Ruben Devlin, Molynsea Inc. · Peter O'Brien, Armunt Design Co. · Sasha Pollar, Molynsea Inc.
On-site meeting · Table 1
Starts in 22 minutes

Thursday, 23 March 2023

11:20 - 11:30 Amy Withe… Pexels Mag…
Online video meeting
Pending · Requ…

Available for meetings?
Indicate your meeting availability by selecting the time slots below. You will only be able to send and receive meeting requests in those time slots.

Wednesday 8 October 2025

☐ Mark all free time slots as available

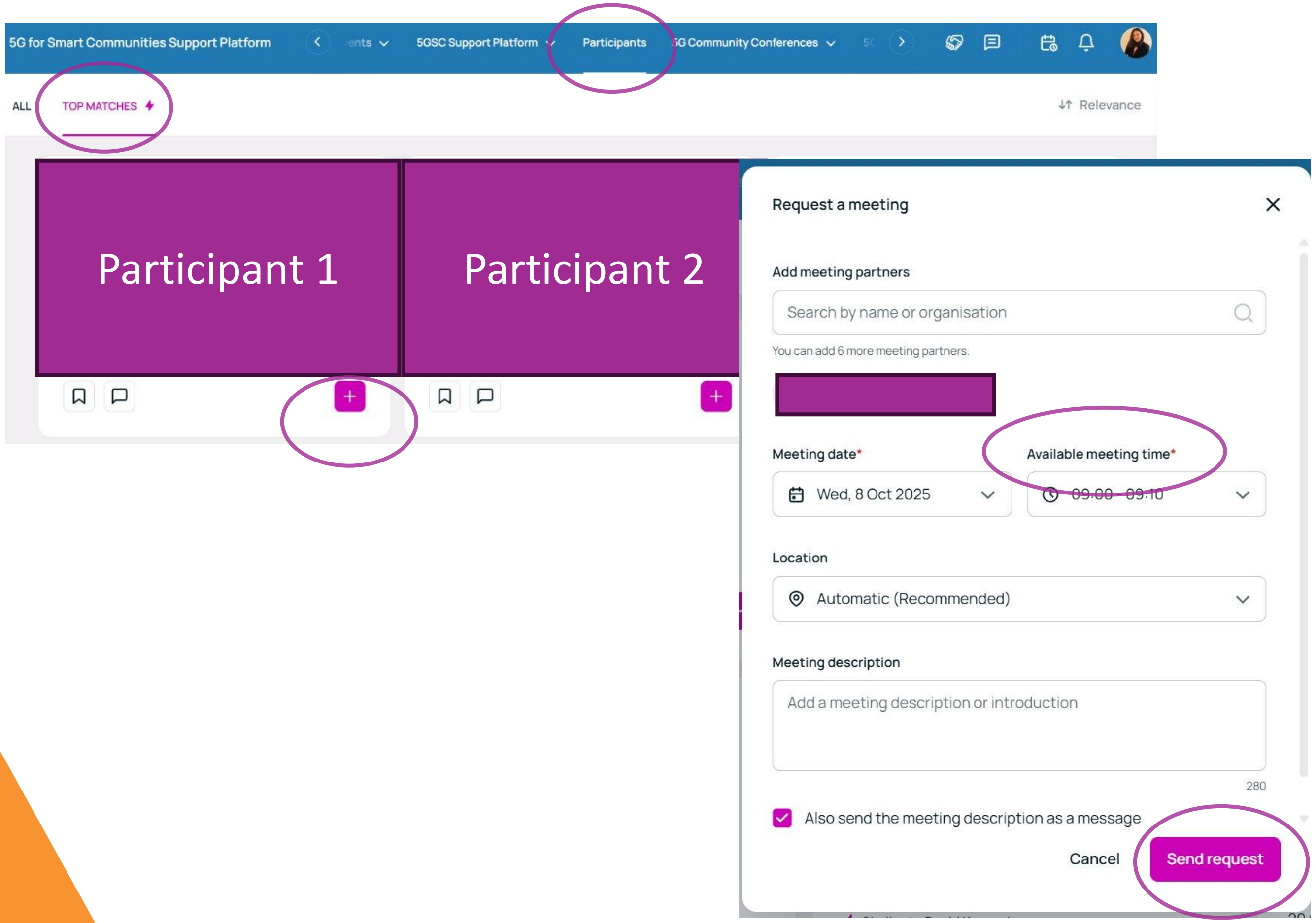
09:00 Overlaps with a session
09:10 Overlaps with a session
09:20 Overlaps with a session
12:20 Overlaps with a session
12:30 Overlaps with a session

Meetings

- ✓ Indicate your meeting availability
- ✓ Click on the slots you prefer
- ✓ Save your availabilities settings

Funded by
the European Union

The 5GSC Platform: Meetings



Request a meeting

Add meeting partners

Search by name or organisation

You can add 6 more meeting partners.

[redacted]

Meeting date*: Wed, 8 Oct 2025

Available meeting time*: 09:00 - 09:10

Location: Automatic (Recommended)

Meeting description

Add a meeting description or introduction

280

☑ Also send the meeting description as a message

Cancel   Send request

Meetings

- ✓ Go to Participants>Top Matches
- ✓ Click on "+" to check availabilities
- ✓ Send the request

Funded by
the European Union

Quantum Technologies in the EU and EuroQCI

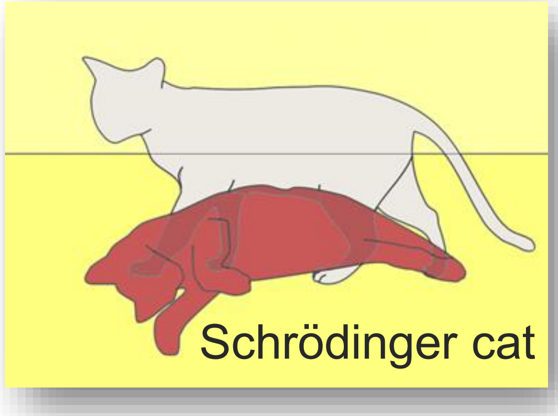
European Commission JRC

Petra Scudo

BroadBandEurope, September 23d, 2025

European Commission

At the basis of quantum tech

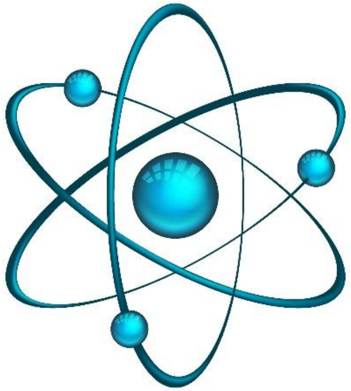

Schrödinger cat

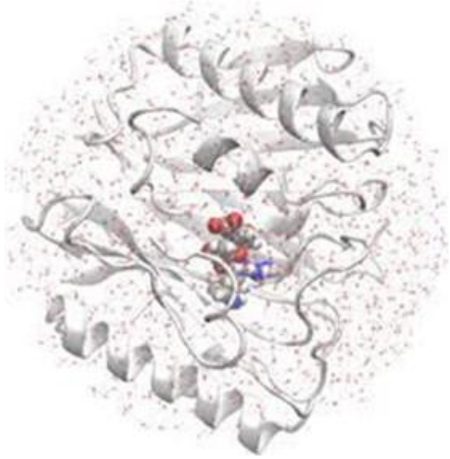
Quantum mechanics describes the behavior of **matter and light at atomic and subatomic** scales

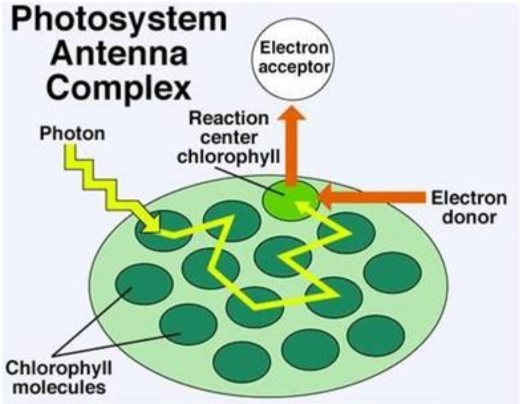
It is often counter-intuitive and in contrast with every-day life observations

100 years of experimental confirmation (founded in 1900-1927)

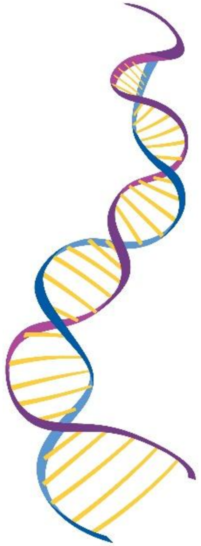
How far does quantum go?

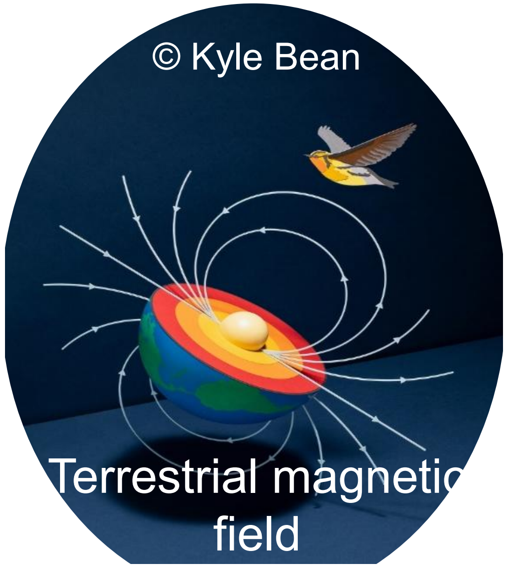

Atom


Protein folding



Photosynthesis

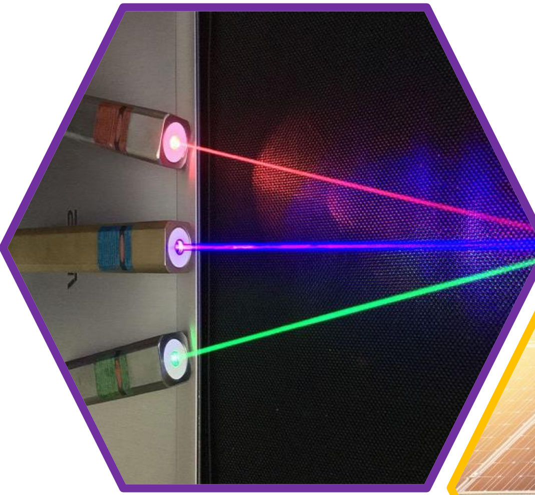

DNA


© Kyle Bean

Terrestrial magnetic field

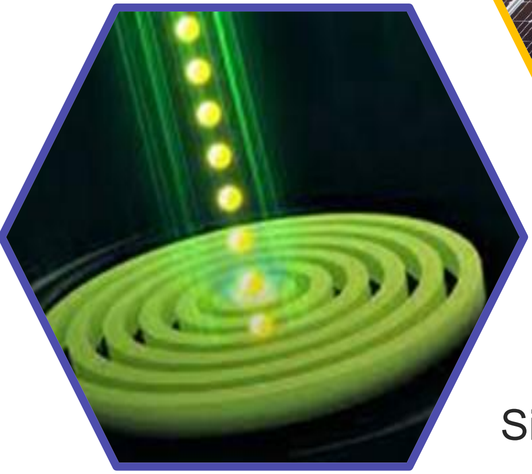
Quantum applications

The unique properties of quantum physics may be exploited in different ways

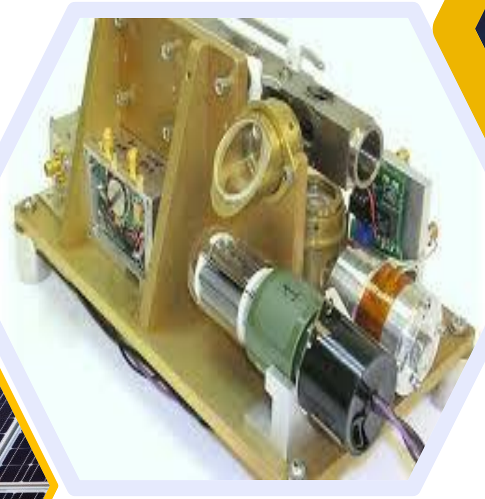


Lasers

Solar cells



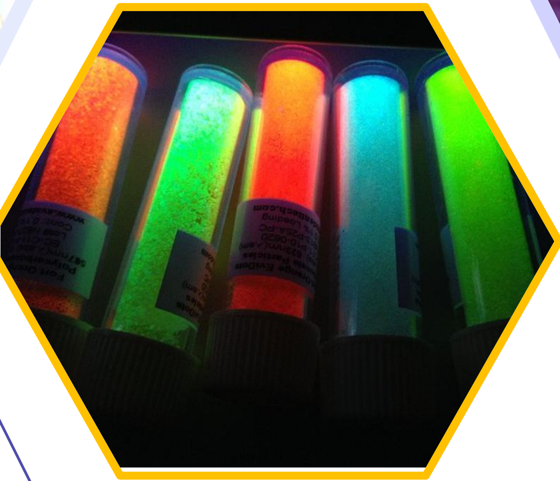
Single photon sources



Atomic clocks GPS

Quantum gravimeters

Satellite based secure keys



Fluorescence

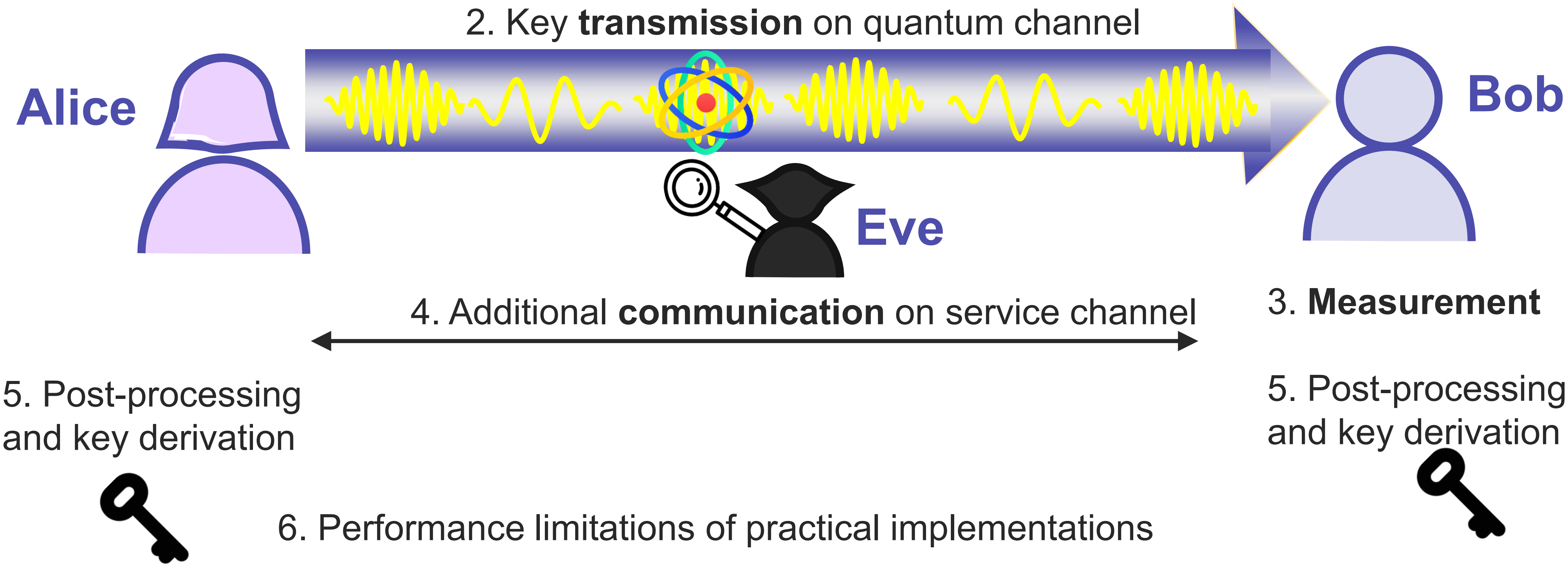
Medical imaging: MRI and PET scans

Quantum Communications

- Quantum communication refers to the use of quantum carriers as physical systems that carry and process information
- Data (bits) can be encoded in quantum states (qubits)
- Quantum states of light particles (photons) can be securely exchanged two parties, e.g., Alice and Bob
- Different quantum information tasks → quantum coding; quantum key distribution; quantum teleportation; quantum error correction, etc.
- Keys used by encryption protocols can be encoded in qubits and securely distributed → quantum key distribution

Quantum Key Distribution (QKD)

1. **Quantum state preparation** e.g. single polarized photons



Alice

2. Key **transmission** on quantum channel

Bob

Eve

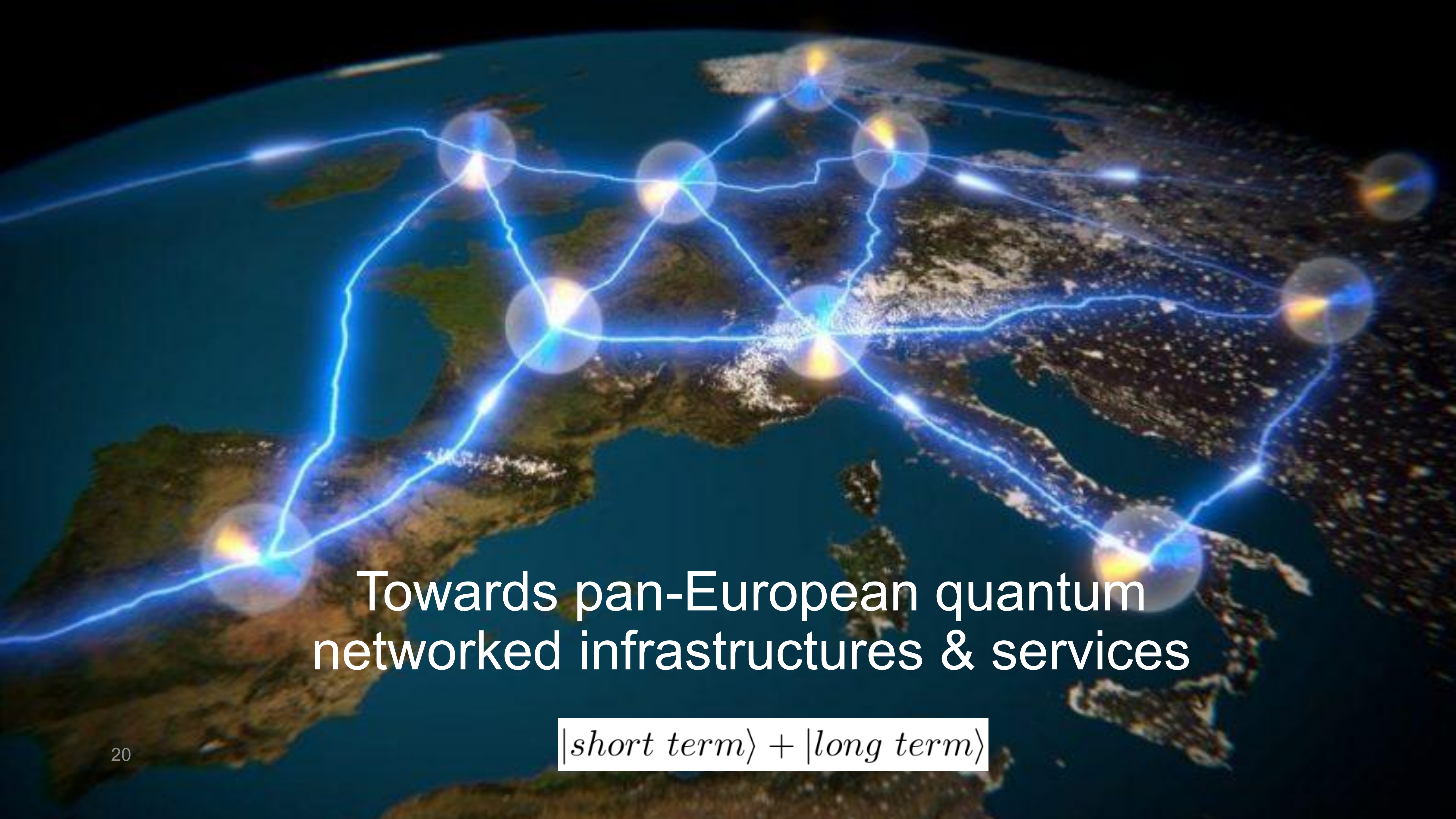
4. Additional **communication** on service channel

3. **Measurement**

5. Post-processing
and key derivation

5. Post-processing
and key derivation

6. Performance limitations of practical implementations
and upper bounds of secret key rates for ground and free space links



Towards pan-European quantum networked infrastructures & services

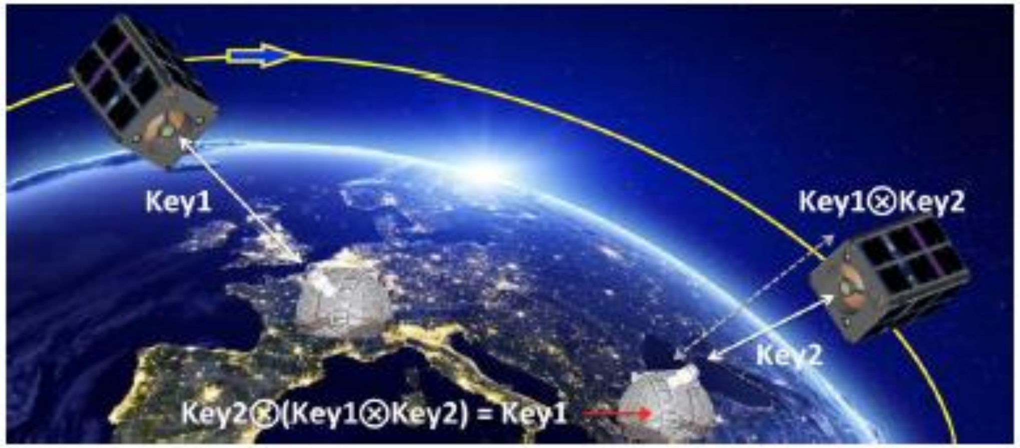
$$|short\ term\rangle + |long\ term\rangle$$

EuroQCI - A governmental QKD service for protection of communications & data and critical infrastructures

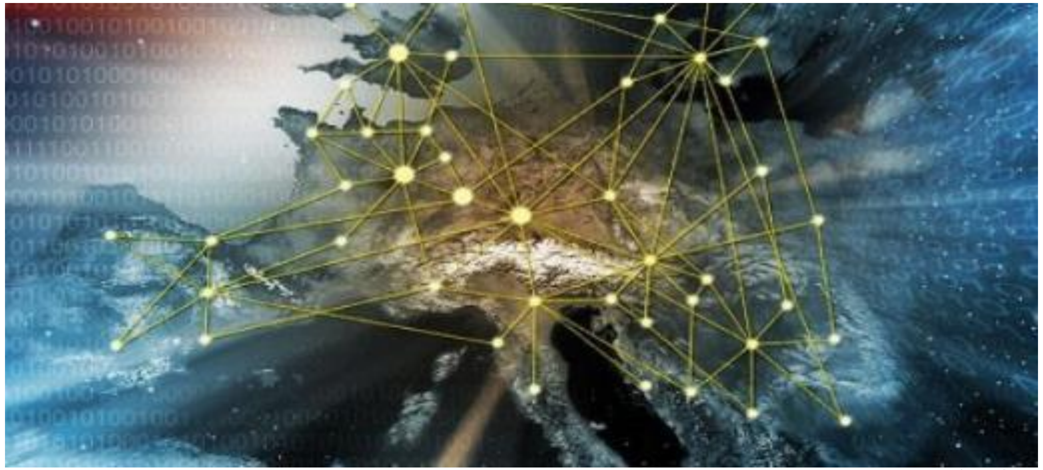
EuroQCI

- An integrated satellite and terrestrial system for ultra-secure exchange of cryptographic keys (QKD)
- Part of the European Cybersecurity Strategy and integrated into IRIS², the Union Secure Connectivity Programme - Regulation (EU) 2023/588

EuroQCI space segment
Distribution of quantum-secured encryption keys on a global scale

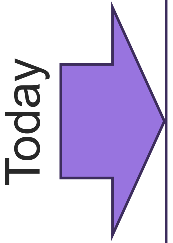


EuroQCI terrestrial segment
Federation of terrestrial QCI networks with cross borders connections



Paving the way to "Quantum Internet", interconnecting quantum computers & sensors

EuroQCI: roadmap



Preliminary validation – demonstration phase

EuroQCI validation

Member States deploy initial QCI networks by 2025 (DIGITAL + CEF)

Space QKD shall be demonstrated in a real environment (Eagle-1)

1st generation: initial capacity

EuroQCI shall deliver unclassified quantum keys for public stakeholders

Reliance only on EU-27 industry

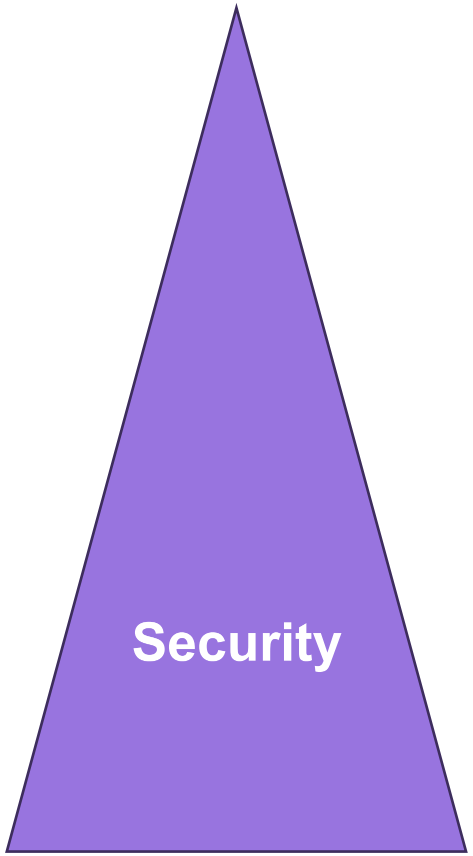
1st generation space satellite(s) - SAGA

2nd generation: final capacity

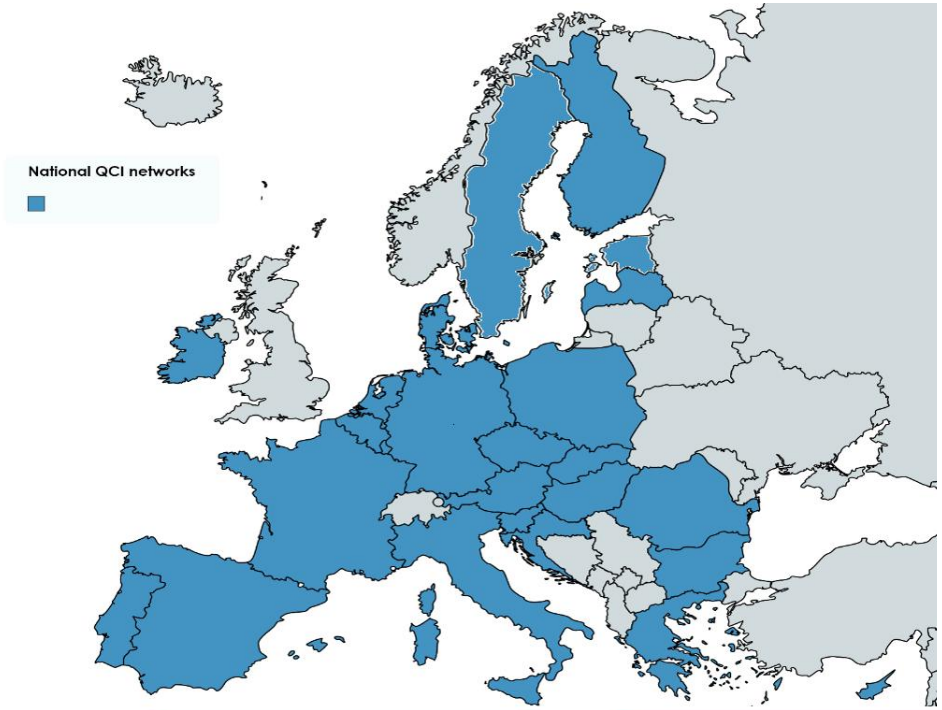
EuroQCI shall deliver quantum keys meeting SECRET UE/EU SECRET

Reliance only on EU-27 industry

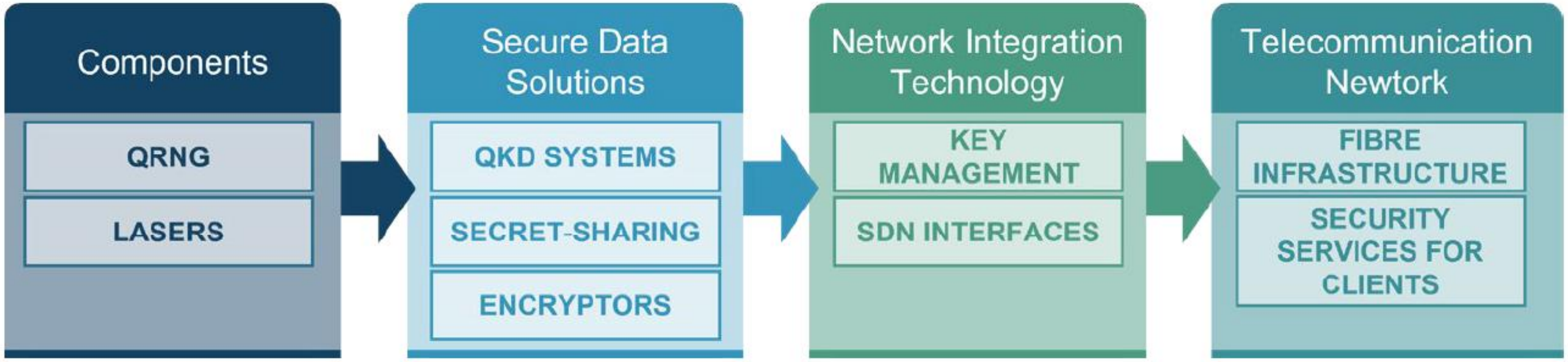
2nd generation space constellation



EuroQCI Terrestrial segment



- 26 Member States deploying national networks (2023-25)
- 6 Industry projects maturing EU QKD technologies (2023-25)
- Deployment of a European QKD product testing and evaluation infrastructure (2024-2028) - NOSTRADAMUS
- Deployment of cross border & optical ground stations for space – CEF call (2026)
- EuroQCI budget: Eur 290 million (160 EU funds) + Eur 138 million space segment + Eur 25 million microsat



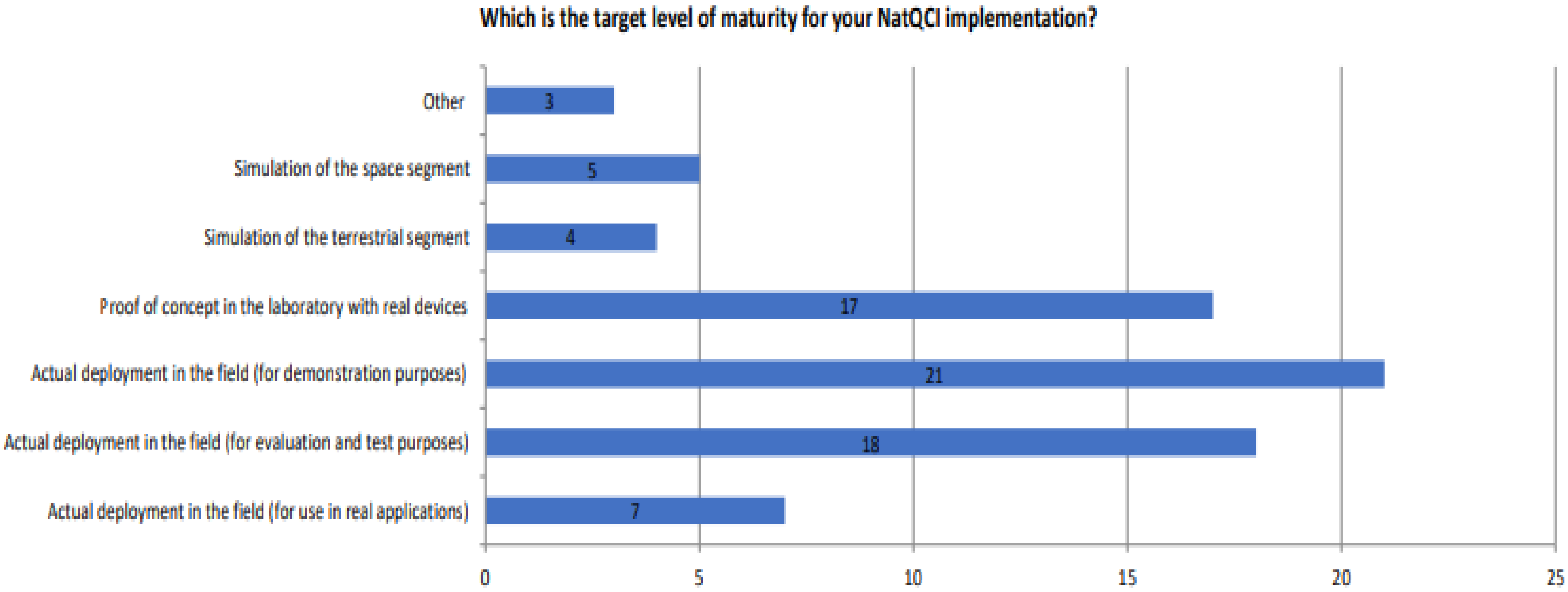
Components
- QRNG
- LASERS

Secure Data Solutions
- QKD SYSTEMS
- SECRET-SHARING
- ENCRYPTORS

Network Integration Technology
- KEY MANAGEMENT
- SDN INTERFACES

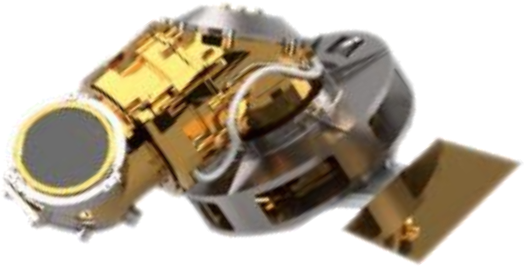
Telecommunication Newtork
- FIBRE INFRASTRUCTURE
- SECURITY SERVICES FOR CLIENTS

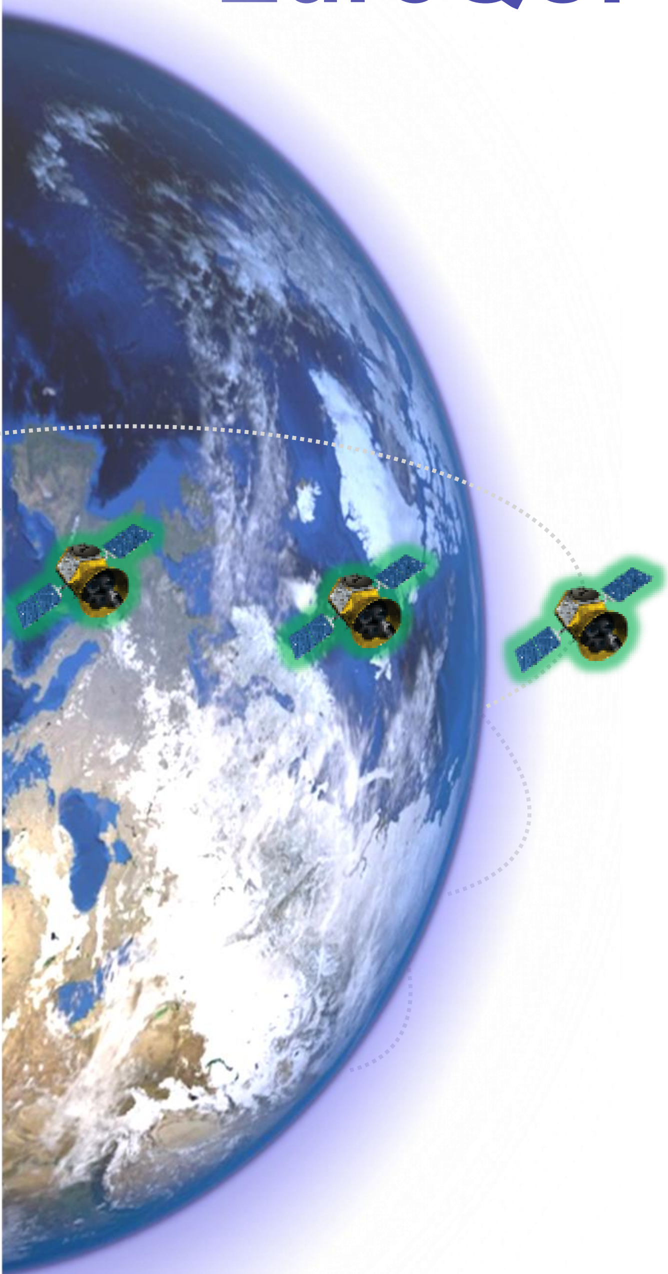
Targets of National projects



Source: PETRUS

EuroQCI Space segment





Eagle 1 – LEO satellite for in orbit demonstration and early tests

- Target launch August 2026
- Funded by Horizon Europe / ESA / Industry
- Operations:
  - QKD proof of concept & testing interfaces with OGS

1st Generation - deployment of LEO satellites with EU technology

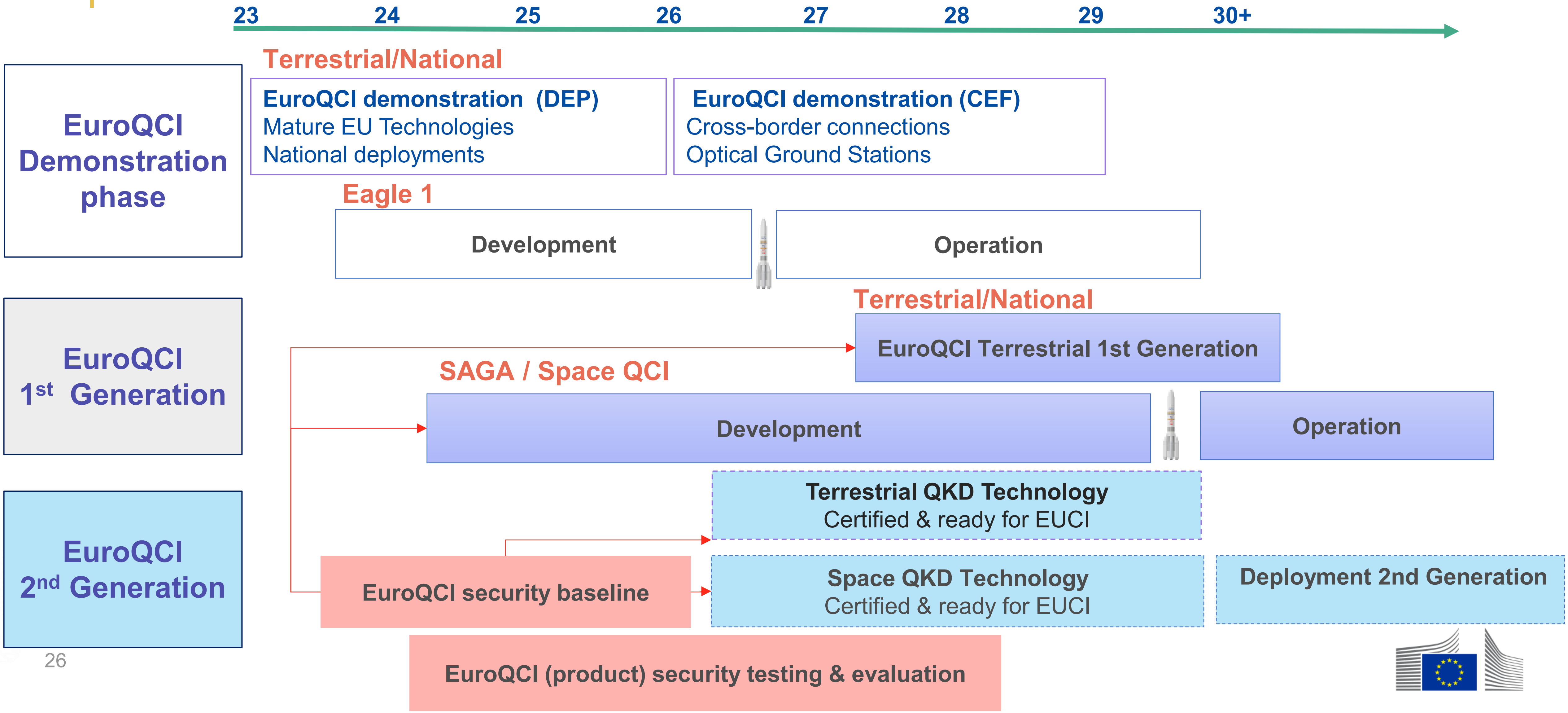
- First prototype satellite by EU & ESA SAGA program
- Possibly additional satellites by Member States
- Operations:
  - Exchange quantum keys between different sites on EU territory
  - First validation of end to end system: interconnected LEO satellites + ground stations + terrestrial systems
  - Initial coverage of user and security requirements – Incremental approach

2nd Generation - deployment of a fully operational system integrated with IRIS² for secure connectivity

Full coverage of user and security requirements

Space & Terrestrial deployment

[work in progress]



23 24 25 26 27 28 29 30+

EuroQCI Demonstration phase

Terrestrial/National

EuroQCI demonstration (DEP)
Mature EU Technologies
National deployments

EuroQCI demonstration (CEF)
Cross-border connections
Optical Ground Stations

Eagle 1

Development

Operation

EuroQCI 1st Generation

Terrestrial/National

EuroQCI Terrestrial 1st Generation

SAGA / Space QCI

Development

Operation

EuroQCI 2nd Generation

Terrestrial QKD Technology
Certified & ready for EUCI

EuroQCI security baseline

Space QKD Technology
Certified & ready for EUCI

Deployment 2nd Generation

EuroQCI (product) security testing & evaluation

Where does Europe stand?

Highest concentration of **talent** (over 100 000 experts, 231 per million inhabitants)

Leadership in scientific **publications** (leading worldwide in some of the fields)

Growing portfolio of **patents** – positive and stable growth in quantum patenting and co-patenting

Strong public **support** (25% global public investments)

~32% of all quantum **companies**

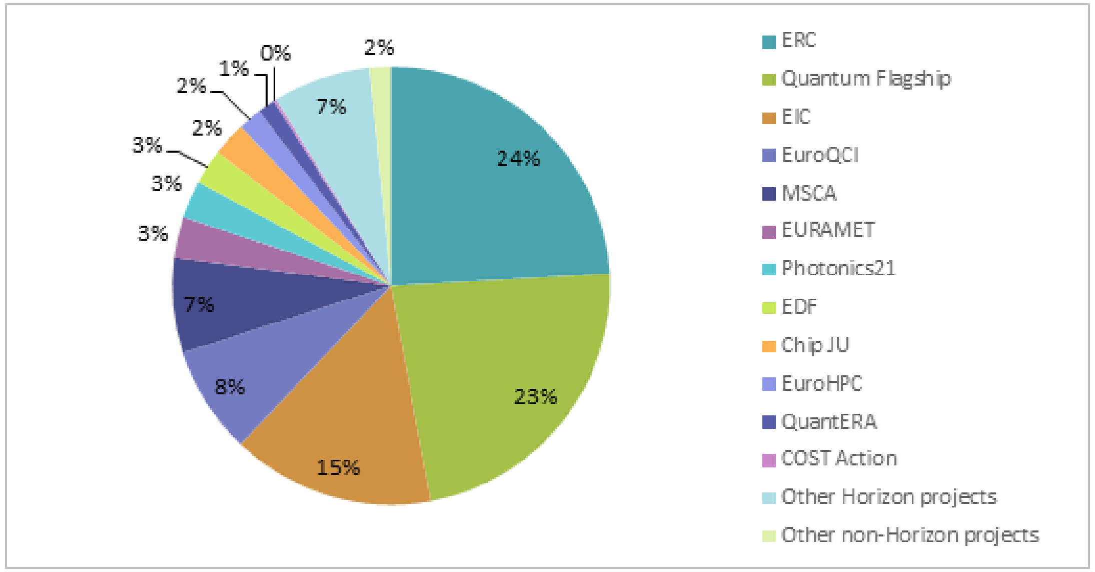
But they only attract ~5% of global **funding**

No EU companies in the top 10 (in terms of quantum investment) - Draghi report

Key Performance Indicators for Quantum Technologies in Europe

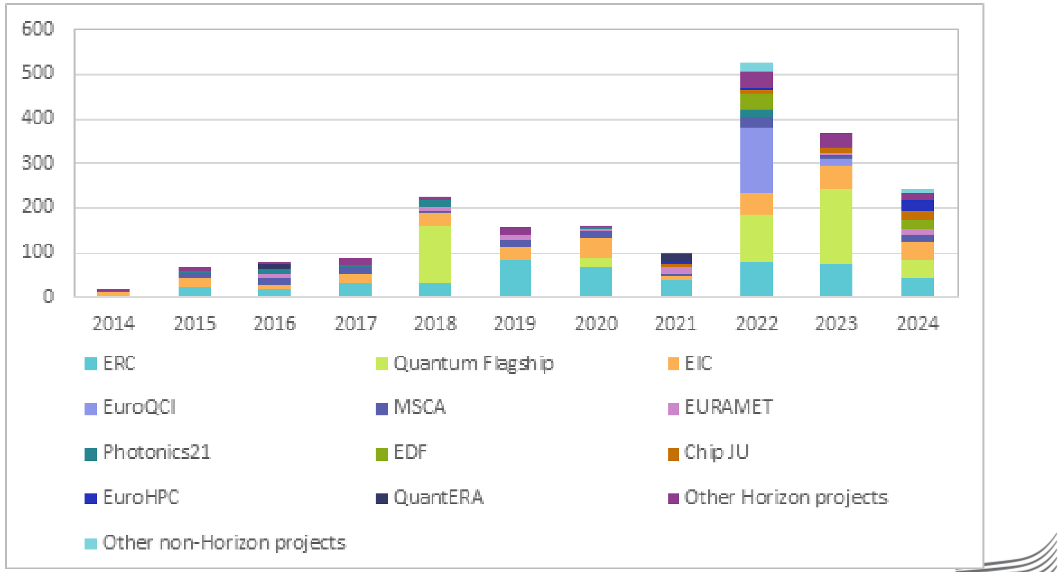
Strategic Research and Industry Agenda

EU public funding of quantum technologies - 1



AI-driven and manual search through CORDIS and EU funding and tenders portal

A total of about 1000 projects identified for a total funding of EUR 2 billion

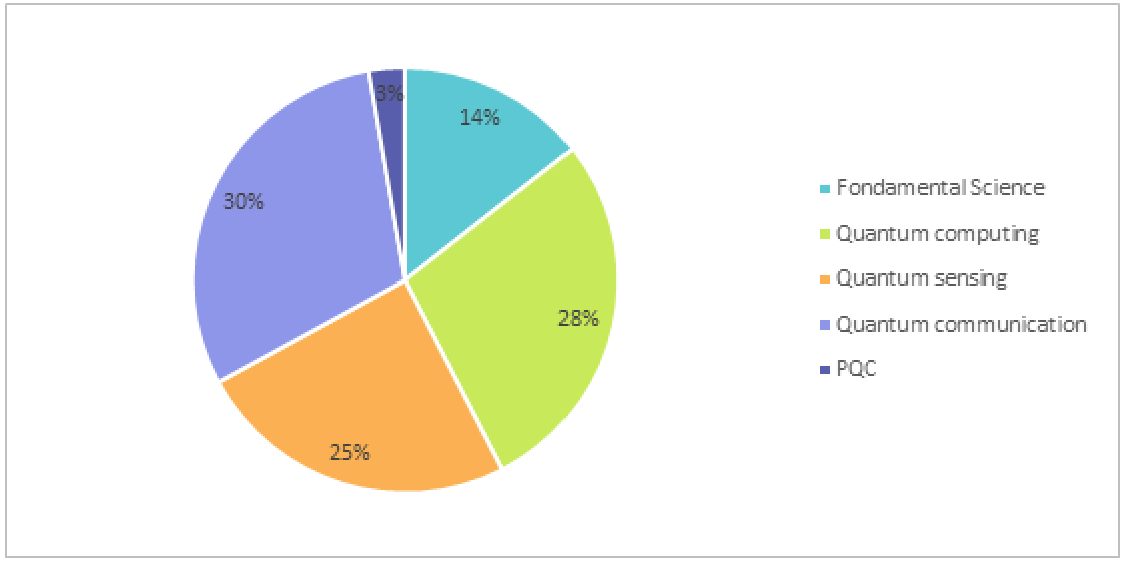


ERC, Quantum Flagship and EIC account for 50% of funding

95% of projects funded under Horizon 2020 and Horizon Europe covering 70% of overall budget

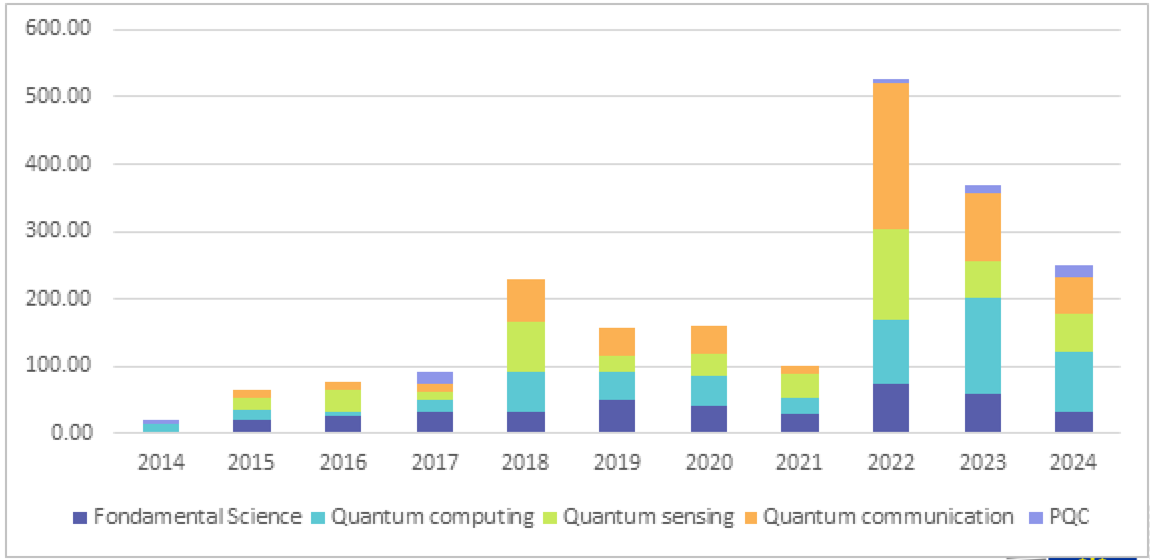
Future directions for Quantum Technology in Europe, JRC 141150

EU public funding of quantum technologies - 2



Identifications of projects by area: fundamental science vs specialized areas – quantum communication; quantum computing; quantum sensing; PQC

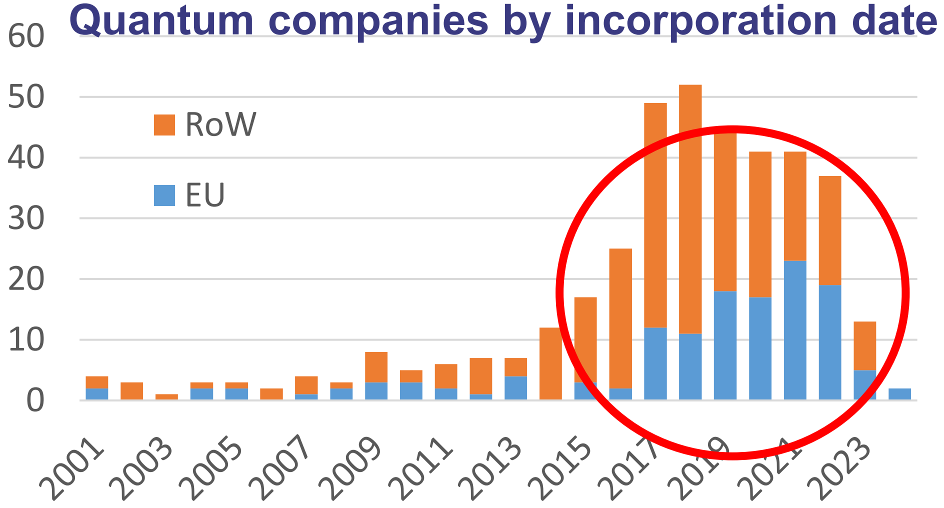
Average funding per project EUR 2.1 million



Global investments in quantum technologies reached about **EUR 36 billion** by end of 2024

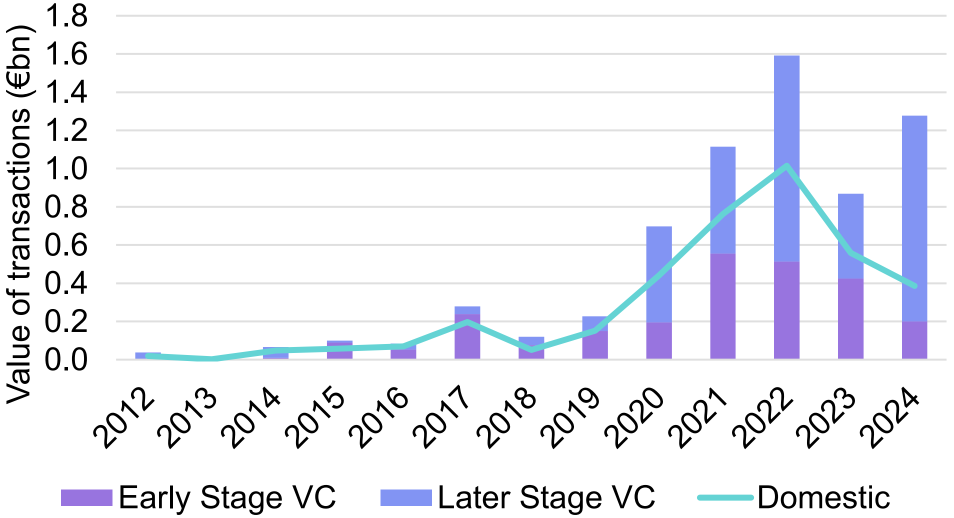
The EU, with **EUR 9 billion**, contributes to roughly **25% of global public funding** (EC, ESA, Member States)

Global landscape of quantum companies



Quantum companies by incorporation date

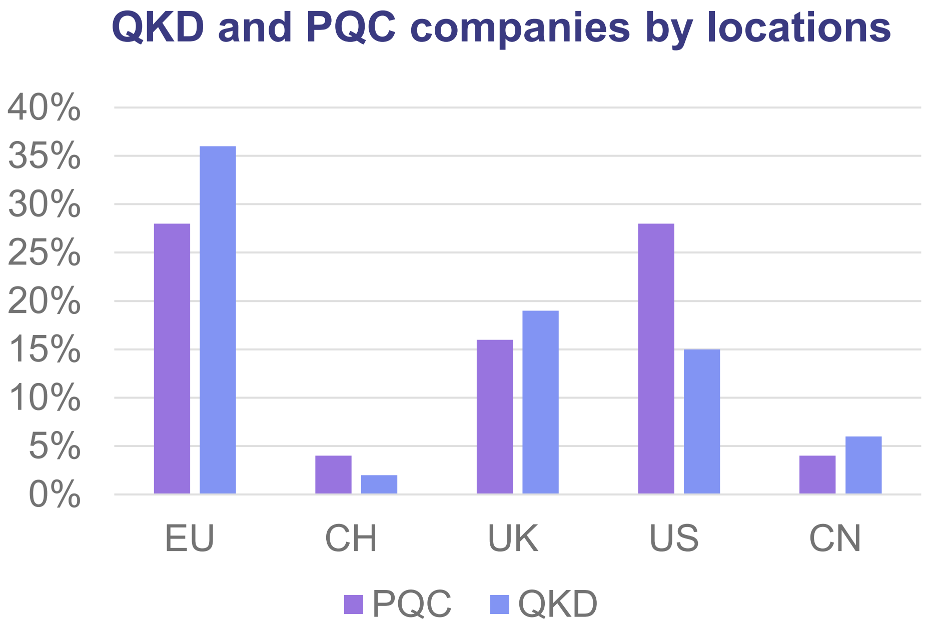
Private investments (Venture Capital)

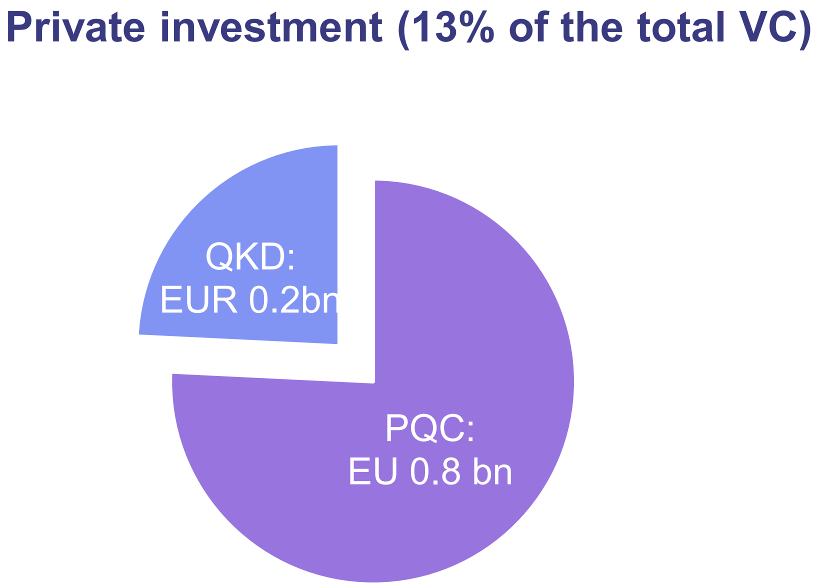


- JRC mapping identified **441 companies worldwide**:
  - ❑ The **EU is home to a 32%** of the total (27% in US and 5% in CN)
  - ❑ **EU firms** tend to **be smaller and younger**: 13% of EU companies classified as large or medium-sized (29% in US and 82% in CN)

- **EUR 6.5 bn of private financing** (VC) and **EUR 40 bn from public sector**:
  - ❑ Private VC:
    - ❑ 61% of the money invested was **later stage VC** (US dominant player)
    - ❑ Recent shift from firm creation to scaling up existing businesses (early-stage venture capital investment decreasing)
    - ❑ Recent shift towards cross-border investments (decrease in domestic investments)
    - ❑ **Private EU investments** started later and **counts 27%** of the total
  - ❑ Public sector:
    - ❑ 34% from CN, 17% from US, and 17% from EU
    - ❑ **EU public program amounts to EUR 2.8 bn**

QKD, PQC: funding

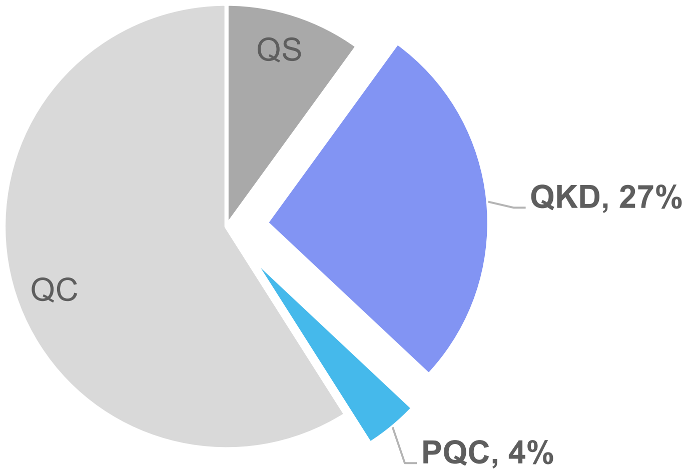




- 25% of quantum companies are in QKD and PQC technology
- **Private investments amounts to about EUR 1 bn** in the last 12 years
- About 32% of EU **public investments** is directed to **QKD** and only a small share to PQC (EUR 3 bn)

QKD and PQC: technology development

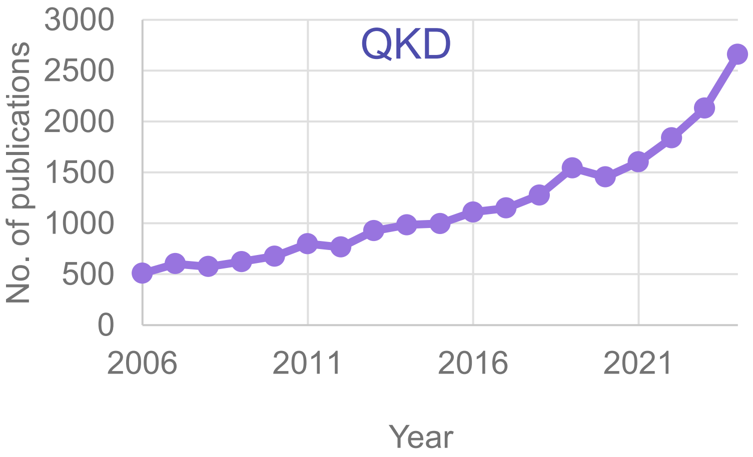
Patents in quantum technology: 30 000

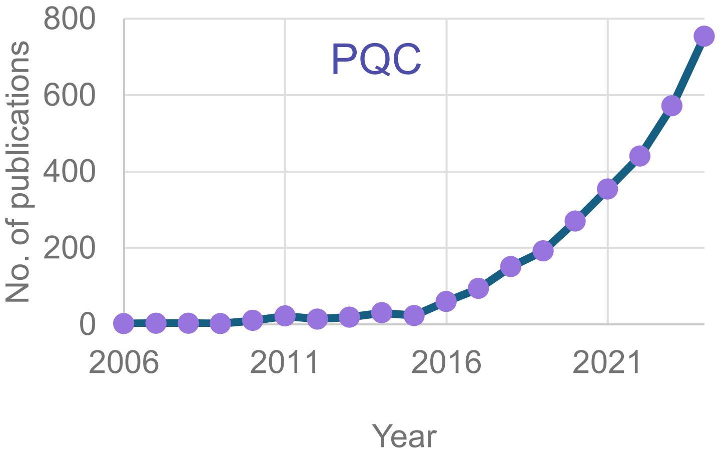


- 31% of **patents** are in QKD and PQC
  - ❑ China holds a significant share (33% in PQC and 46% in QKD)
  - ❑ The EU is contributing to the field, ranking fourth (9% in PQC and 6% in QKD).
  - ❑ EU co-patenting higher than in other jurisdictions: 8% for PQC and 21% for QKD (mainly with EU)

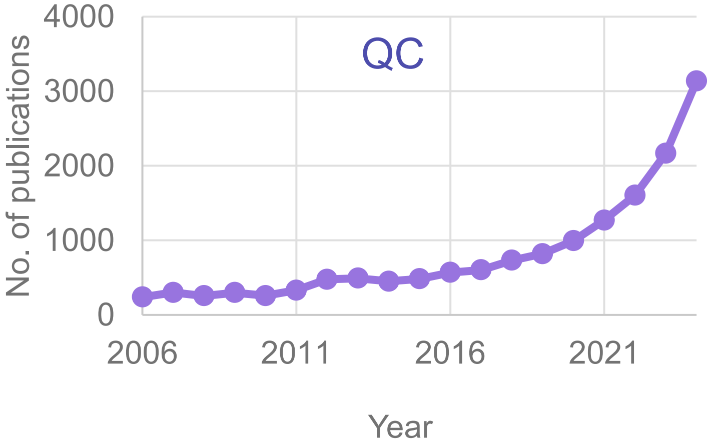
Scientific and technical publications

Keywords query of Scopus database – quantum communications (QKD, PQC), computing (QC), and sensing





- QKD publications worldwide, 2006-24
- The number of publications tripled in about 12 years, 2013-2024
- For QKD, the main affiliation country is China closely followed by EU
- For PQ, the main affiliation country is EU, followed by USA and China



Publications in quantum computing increased by over 6 times in the last 10 years, with a CAGR of 27% as from 2017

Publications in quantum sensing grew similarly,
very much related to specific sub-area,
the greatest being for NV and Rydberg atom sensors

Standards for QKD

JRC is Commission representative on:

- ETSI ISG QKD
- ETSI TC CYBER Quantum Safe
- CEN CENELEC JTC22
- IEC/ISO JTC3

→

Standardization Roadmap on Quantum Technologies
New edition just released

Nostradamus and JRC Quantum Lab

- EuroQCI project funded under DEP (partners DT, AIT, Thales)
- CNES Toulouse lab to be transferred to JRC in 2027
- Quantum hacking attacks to be tested
- Nostradamus' priority testing based on triplets: QKD product, QKD protocol, side channel attack
- Roadmap to QKD certification under EUCC scheme by a National Certification Body
- Evaluation by and ITSEF + ISO 17025 accredited laboratory

Certification framework for EuroQCI

- **Existing EUCC**

  SOG-IS list of ITSEFs

  each accredited up to a defined EAL

  accredited to ISO/IEC 17025 and apply ISO/IEC TS 23532

- **Proposal for EuroQCI**
  - CC certification using ETSI PPs by an ITSEF accredited to EAL4+
  - ITSEF subcontracts JRC to carry out QKD-specific tests
  - JRC ISO/IEC 17025 accredited for these tests

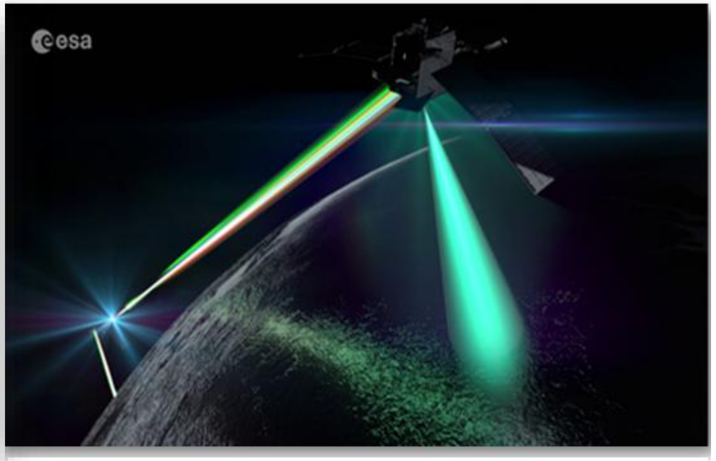
- Trust!

- *Any certification for classified information is by MS*

- Staffing: Commission staff
- NOSTRADAMUS and subcontractors
- ITSEFs
- NMIs

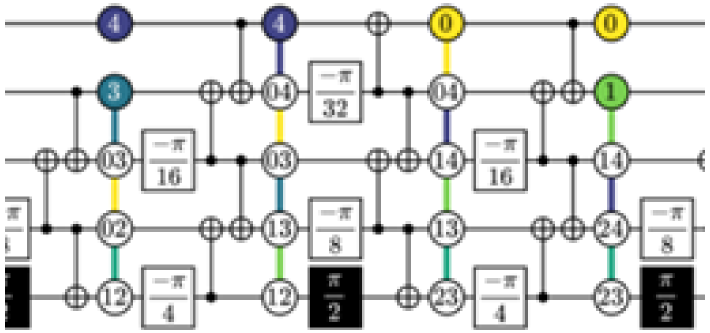
JRC’s activities in Quantum Technology

Quantum communication: on-site testing of QKD equipment and installations



Quantum security analysis and proof of the quantum space link (ESA)

Quantum sensing for space and defence

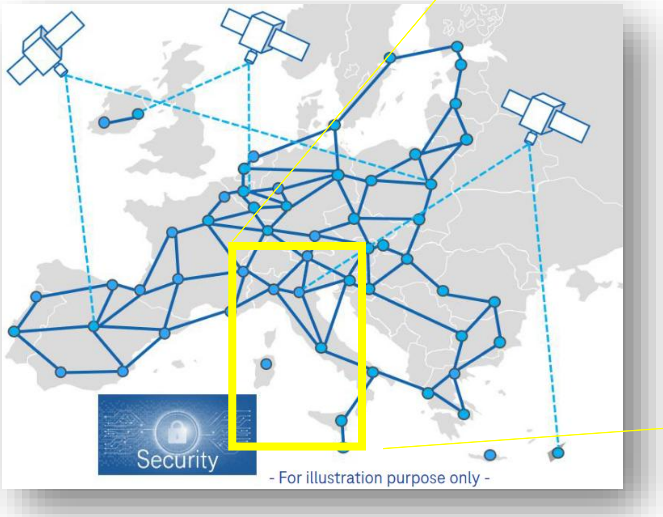


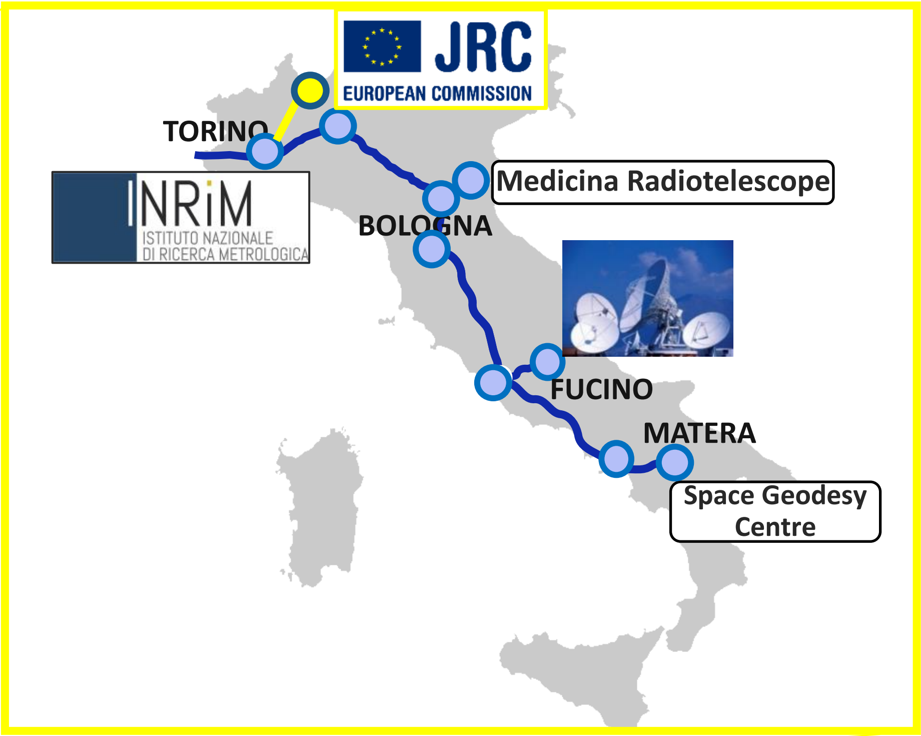
Quantum computing algorithms for practical applications

JRC connected to EuroQCI through the Italian Quantum Backbone

Distribution of

- timing signal
- quantum signals (QKD)





Quantum @ JRC 2025

communications

JRC Quantum Lab

Connecting to the Italian Quantum Backbone via INRIM

JRC Quantum Policy Report (soon to be published)

JRC/ESA quantum security for EuroQCI space

EU role in Quantum global race', Science for Policy Briefs

computing

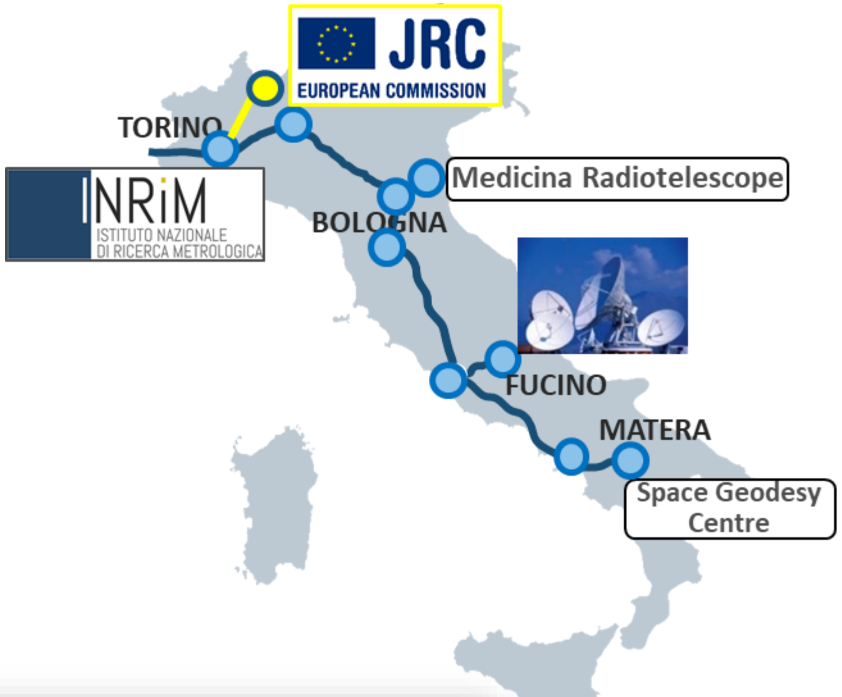
JRC/CERN collaboration on quantum computing

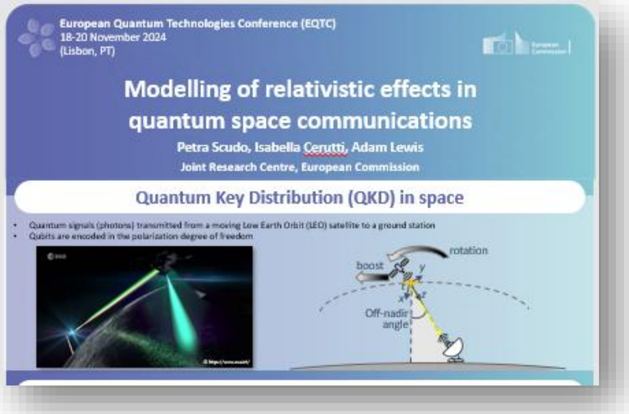
Monte Carlo and Quantum Algorithms for optimization of radio spectrum links

New algorithms quantum machine learning

sensing

Supply chain monitoring





European Quantum Technologies Conference (EQTC)
18-20 November 2024
(Lisbon, PT)

Modelling of relativistic effects in quantum space communications

Petra Scudo, Isabella Cerutti, Adam Lewis

Joint Research Centre, European Commission

Quantum Key Distribution (QKD) in space

- Quantum signals (photons) transmitted from a moving Low Earth Orbit (LEO) satellite to a ground station
- Qubits are encoded in the polarization degree of freedom

Thank you

Slide xx: element concerned, source: e.g. Fotolia.com; Slide xx: element concerned, source: e.g. iStock.com

Generalitat de Catalunya
Departament de la Presidència
Secretaria de Telecomunicacions
i Transformació Digital

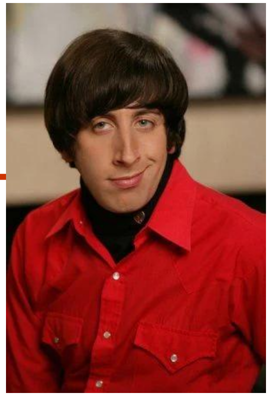
Quantum in Catalonia

Design and tendering for a public quantum network

September the 23rd

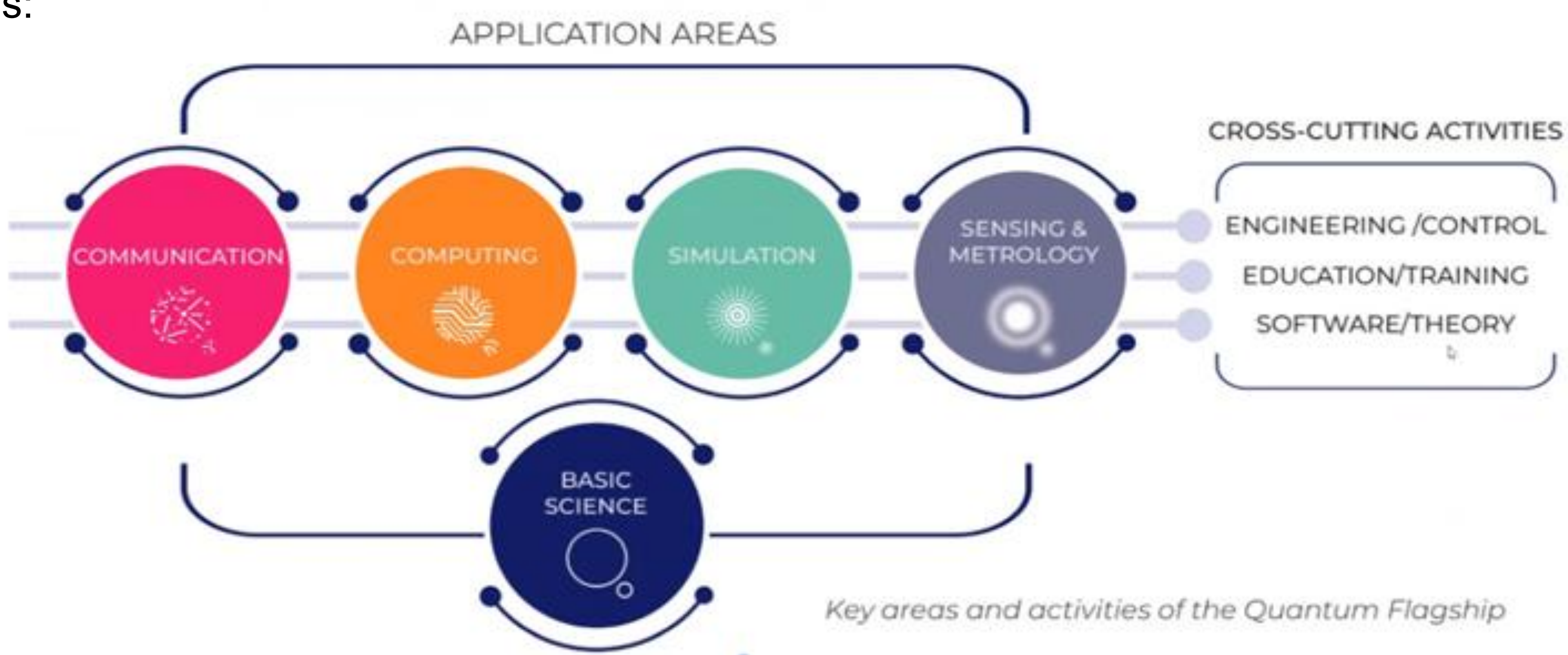
BCO Network

Quantum for engineers (1/2)



Application areas of Quantum Tech (Today, 2025)

Main areas:



Key areas and activities of the Quantum Flagship

Quantum for engineers (2/2)

Quantum is used for... (very simplified)

- **Quantum Detection.** Ultra-precise measurements, which will have disruptive applications in natural resource management and medicine.
- **Quantum Computing.** Powerful fault-tolerant universal machines may be years away. Small but useful special-purpose quantum computing devices are now available.
- **Quantum SW**. Completely new SW for quantum computers or simulations on traditional HW systems (computers, HPC).
- **Quantum Materials**.
- **Support Tech.** Mechanics, cryogenics, vacuum techniques or photonics.
- **Frontier science.** Dark matter, transition from atomic systems to mesoscopic phenomena, role of quantum laws in general and randomness in particular.
- **Other Tech.** Quantum technologies should find important applications in traditional technologies, products and services.
- **Quantum Internet.** Explained later in this document.
- **Quantum Cybersecurity.** Explained later in this document.

Quantum communication (1/3)

Fibre Optical network, but also...

Quantum communication aims to distribute quantum states and quantum resources (such as qubits and entanglement) between remote parties. The security of data encryption would not be based on mathematical complexity as it is now, but rather on the intrinsic randomness of quantum physics. It is impossible to copy a quantum state (and therefore quantum information) without introducing errors, which allows the user to **immediately detect when a communication channel is attacked**.

These advanced quantum networks could also be used to carry out "***Blind Quantum Computing***", that is, to execute calculations on quantum computers in which all the information would be inaccessible even to the computer itself that is doing the calculation. A relevant aspect to consider in this objective, for a sustainable development of quantum communication, is its integration into the network infrastructure in coexistence with classical systems.

Quantum communication (2/3)

Actual reality (2025)

The first-generation technology for quantum cryptography has already reached **commercial products** and prototypes for quantum random number generation (**QRNG**) and quantum key distribution (**QKD**) already available. In Europe, these technologies are being commercialized by Quside and Luxquanta, respectively. In addition, fiber optic networks for QKD have been built in several territories, including Europe, the USA, China and Japan.

China, Europe, Canada and the USA, among others, have a program to develop and launch satellites for quantum communication. However, only China has made real demonstrations so far.

Optical fiber quantum network: 200 -1.500 Km

Satellite communications (secured global network)

Quantum repeaters (***still under development***)

Quantum communication (3/3)

Quantum networks actual development (2025)

The main technical limitation is that quantum information is carried by individual photons and that losses in optical fibers increase with distance. For terrestrial quantum communication on a scale beyond the metropolitan area (hundreds to thousands of km), trusted nodes can be used that lead to a sequence of secure links.

An alternative to trusted ground nodes is to use a satellite as a quantum transmitter. Depending on the QKD protocol, the satellite may or may not act as a trusted node for ground-based communication links.

In the long term, quantum repeaters will be developed, offering secure communication independent of the reliability between nodes, beyond metropolitan distances. In fact, quantum repeaters and satellites are complementary and necessary to distribute resources such as entanglement over long distances for more complex applications.

Quantum networks main improvements needed

Quantum repeaters. Quantum repeater elements for fiber communication have been demonstrated by research groups with different systems within the laboratory and between different laboratories. However, we are still far from building a fully functional prototype that demonstrates advantages over direct communication and is deployed in the field. Further research and development is needed, as well as the creation of the first deployable prototypes.

Satellite communication. Satellite-based quantum communication is done using telescopes that share single photons, which means that the link is very sensitive to background light and scattering. Therefore, it often has to operate at night and in clean environmental conditions. In Europe there are groups developing technology for quantum communication using satellites, both geostationary (GEO) and low-orbiting (LEO), including nanosatellites such as cube-sats.

Post-Quantum Cryptography, PQC (1/3)

Assumption: **Classical vs quantum encryption (BCO Network meeting in Zagreb, 2025, June, the 11th)**. Actual encryption based in mathematics is vulnerable with quantum computing.

To address this risk posed by quantum computers, NIST initiated a project in 2016 to define new asymmetric cryptographic standards based on alternative mathematical problems to those already known, with the ability to be robust against quantum computing. These algorithms are known in the literature as post-quantum cryptography (PQC), and they will work over traditional computers (and HPC).

On March 11th, 2025, NIST announces the Fifth Algorithm for Post-Quantum Encryption that completes the needed basic tools to implement PQC in classic networks with quantum encryption cybersecurity.

Post-Quantum Cryptography, PQC (2/3)

PQC expectations

The implementation of Post-Quantum Cryptography (PQC) is expected to restore data security to its current state, prior to the advent of quantum computers, once the initial challenges are overcome. These challenges include problems related to hardware implementation (PQC algorithms have different requirements than current ones in terms of key size, storage, computational resources, etc.) and vulnerabilities of the algorithms. However, the security provided by PQC will continue to depend on advances in the mathematical and computational capabilities of both classical and quantum computers.

It should be mentioned that with the widely used RSA algorithm, it has been necessary to constantly update the key size for several decades to keep up with the growth of computational power. However, with the advent of quantum computers, RSA needs to be replaced because increasing the key size no longer helps prevent attacks.

Post-Quantum Cryptography, PQC (3/3)

PQC problems in actual networks

Apply PQC is not just apply PQC algorithms in the application layer (change RSA to PQC).

In an end-to-end use case, between the application and the browser there are intermediate elements (balancers, gateways or browsing proxies, corporate browsing IPS, etc.) that apply cryptographic directives. It is necessary to achieve the migration of each of the elements in the chain that apply crypto to have a transformed environment to PQC.

It's expected a migration of actual systems to PQC and the coexistence of PQC and QKD till a complete migration to quantum networks.

Quantum Key Distribution , QKD

State of the art

They base their security on the basic principles of quantum mechanics and not on the strength of a mathematical problem or on assumptions about the computational capacity of an adversary.

An example of one of the main challenges currently encountered in quantum cryptography is the certification of devices and compatibility with the existing communications infrastructure. Despite the technological challenges, in the field of quantum cryptography there are already commercial devices that implement one or more quantum key distribution (QKD) protocols and that are already being successfully applied in industry (with high TRLs).

As a prominent example of global progress, China has demonstrated a large-scale quantum key distribution network integrating ground nodes with links between satellites and ground stations. Similarly, Europe has launched the EuroQCI project, which aims to establish a QKD network between member States in the next decade to protect critical infrastructure.

Quantum communication QKD (1/2)

Terrestrial Communications (o.f.)
Aerial (drones, between drones 1Km)
Satellite (LEO, 4.600 Km)
Subsea cables (Lab tests)

Scenarios quantum communication (QKD and KMS elements)

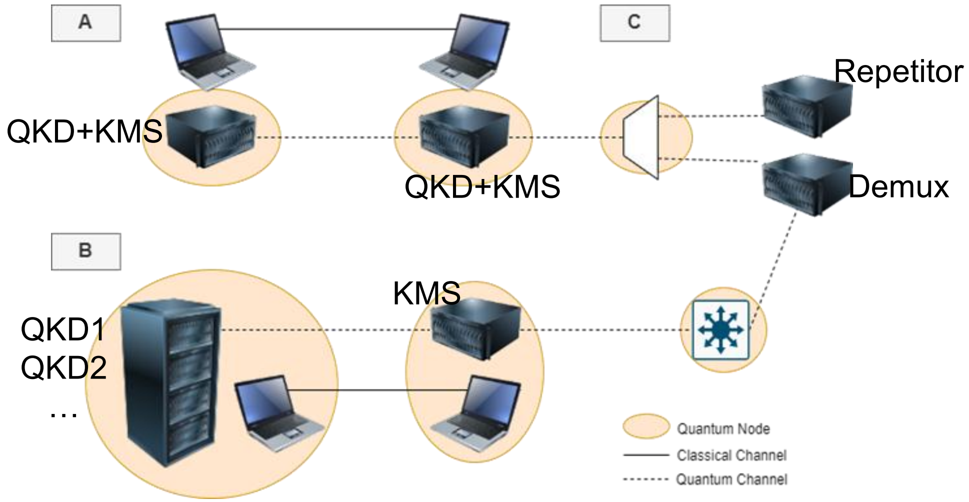
Quantum nodes. A quantum communications node is a physical location capable of generating secret symmetric keys using QKD with another quantum node. In general, and as discussed in the next section, each node consists of one or more QKD equipment and a key management system (KMS). These nodes can have different functions and key generation capabilities.

Scenarios

A. Simple direct communication.

B. Multiple QKD, One KMS.

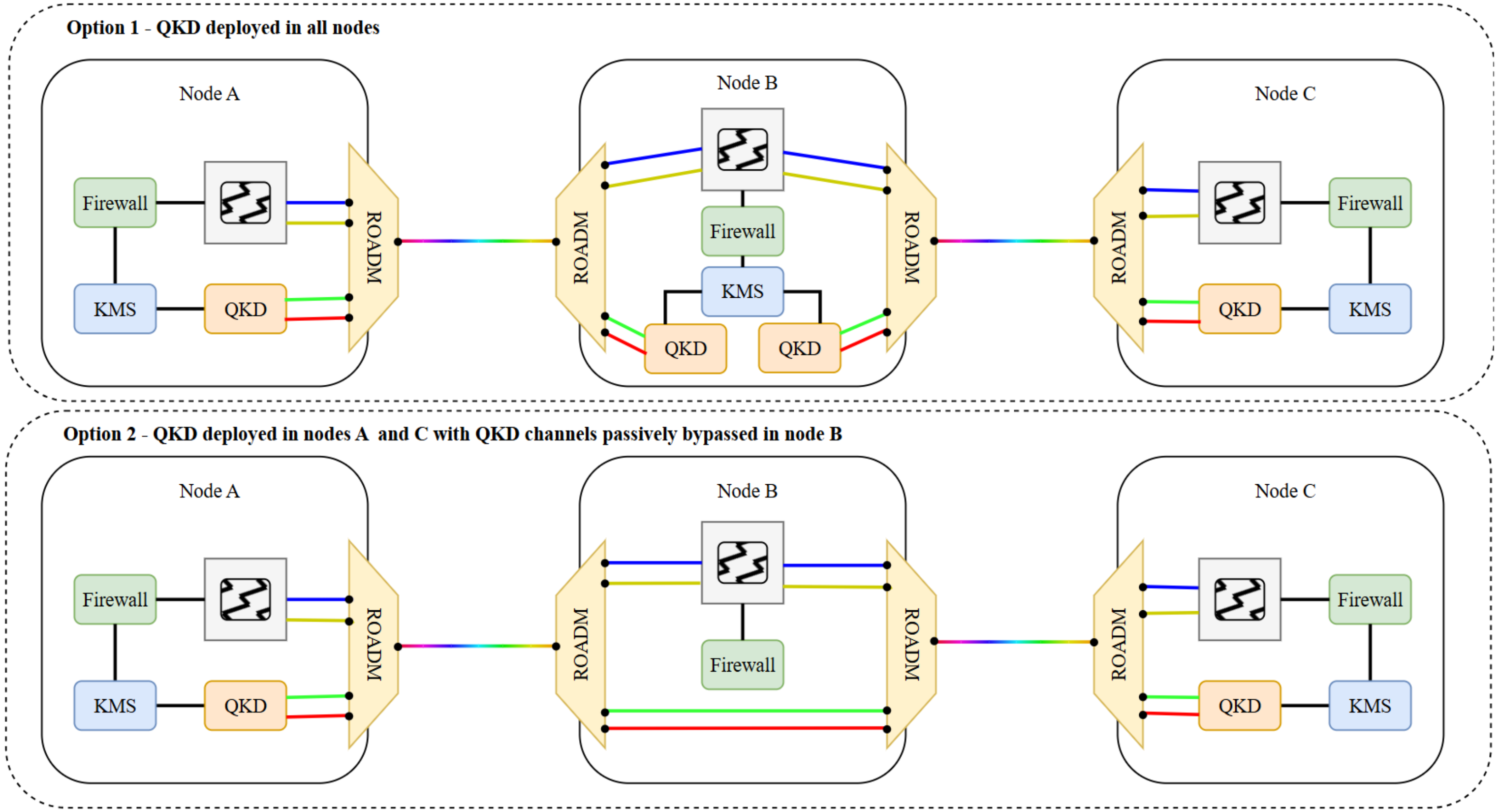
C. Intermediate nodes (just repeat or demultiplex).



Generalitat de Catalunya
Departament de la Presidència
Secretaria de Telecomunicacions i Transformació Digital

Quantum communication QKD (2/2)

Multiple nodes QKD (This can only be implemented if the total losses of the MUX/DEMUX link do not exceed the maximum permissible for the QKD system)



QKD commercial systems (1/3)

DV-QKD & CV-QKD

QKD systems represent a **mature quantum technology** that is already deployed on a small scale at a commercial level in multiple sectors, both public and private, demonstrating its utility and reliability in real scenarios.

This scenario is encouraging new companies to launch themselves on the market with innovative proposals, joining the established manufacturers that, for years, have developed and evolved successive generations of QKD solutions. The result is **different QKD protocols** that result in technological versions with different performances. However, these performances are limited by the characteristics of the receiver used, which allows classifying all the technologies into two large groups: Discrete Variable (**DV-QKD**) and Continuous Variable (**CV-QKD**).

QKD commercial systems (2/3)

DV-QKD and CV-QKD

DV-QKD require single photon detectors at the receiver. These detectors are expensive, need to operate at very low temperatures, and cannot be integrated into integrated photonic circuits. Good for satellites/drones (highlights the manufacturer IDQ, Swiss company, ID Quantique).

CV-QKD It uses coherent detection, a technology similar to that used in current optical communications systems. This makes it possible to take advantage of mature and widely available components in the telecommunications field, known as telco-grade (three manufacturers in the world commercializing solutions, the Catalan company LuxQuanta stands out, as the first to launch a commercial product and with the largest number of systems deployed).

Choose one or the other will depend on: Looses on **dB** (taking into account all elements of the link); **secret key rate** (kbps, asymptotic key rate or final key rate –real measurements-, speed at which secure information can be shared between parties); **co-propagation capacity** (ability of a QKD system to coexist and operate simultaneously with classical telecommunications channels within the same fiber optic infrastructure); **costs** (€).

QKD commercial systems (3/3)

	DV-QKD	CV-QKD
Tech	single photon detectors (can not be integrated in QKD chips), -40ºC or -30ºC	standard telco grade coherent detectors
dB	between 100 km (20 dB) and 830 km (140 dB)	80 km (18 dB)
secret key rate	In satellite or long distances, not so critical. It is in metropolitan areas.	100 kbps short distances (10-20 km) and lower long distances. Actually, no limitation in real systems, but to be aware in future big implementations)
co-propagation capacity	In optical fibre, use O band because of noise of classic comms (higher looses, but less noise). Use of dedicated optical fibres	Uses same C band as classic optical communications
€	High (few prospects for cost reduction and technological scalability, -30ºC)	Approx. 30% lower than DV-CQKD (equipment) and easy integration. Expected cost reduction in line with market growth

EuroQCI

2019-2027 programme

Since June 2019, the 27 EU Member States, in collaboration with the European Commission and the European Space Agency, have worked on the development of EuroQCI, a quantum communication infrastructure that will cover the entire EU. Terrestrial and satellite network.

Linked to IRIS, transition to quantum cryptography recommendation, cybersecurity strategy, etc.

Different Member States are building their networks and connecting them to EuroQCI.

Main EU funding infrastructure Programmes: EuroQCI, DEPs-Infra, EuroHPC JU (EuroQCS).

Other important national initiatives are Quantum Spain, Munich Quantum Valley (MQV), Quantum Delta NL (Nederland), Danish Quantum Community, Quantum Austria, France Hybrid Hpc Quantum Initiative (HQI), WACQT (Sweden), Quantum Portugal, Italian National Center for HPC, Big Data and Quantum Computing (Italy), etc.

Catalan ecosystem (1/3)

Why Catalonia? Research

ICFO: It has participated in a total of 182 projects related to quantum technologies since 2010, of which 68 have been funded by the European Commission. Among these, the projects of the European Research Council (ERC), the European Innovation Council (EIC) and the **Quantum Flagship** stand out. Infrastructures, labs, spin-offs (Luxquanta, Quside, etc.).

UB: ICCUB (comp, comms) / Magnetism (materials) / IN2 (comp) / etc.

UAB: Optics (comp, materials, comms) / GIQ (comp, comms, sensors) / Nanocomp (comp), etc.

UPC: GCO (comp, comms) / N3Cat (comp, comms) / Bampla (commms, sensors), SPCOM (comms, comp) / BQMC (comp, sim, sensor, materials) / DONLL (comms) / etc.

BSC: Comp, spin-offs: Quilimanjaro (BSC-UB).

Among others (IFAE, ICN2, I2Cat, CTTC, IMB-CNM, Eurecat, IEEC, etc.)

Catalan ecosystem (2/3)

Why Catalonia? Spin-offs

Quside Technologies S.L.: Quantum random number generation for commercial terrestrial and satellite systems. Hardware acceleration of randomized computational techniques (comp, comms).

LuxQuanta Technologies S.L.: Quantum cryptographic key generation and distribution. Terrestrial Quantum Cryptography with Continuous Variable Technology (CV-QKD) (comms).

Qilimanjaro: Remote Analog Quantum Computing Services "*Quantum as a Service*" (QaaS). Co-design of hardware and software "*Quantum ASIC*" (QASIC) solutions for specific use cases. Deployment, integration and maintenance of digital and analogue quantum computers (comp).

Catalan ecosystem (3/3)

Why Catalonia? Government support (1/2)

QunatumCAT (RIS3Cat, Smart Specialisation Strategy, ERDF Funds), is a hub of research institutions in Catalonia (ICFO, UAB, UPC, UB, BSC, ICN2, I2CAT, IMB-CMN, CTTC, IFAE) and industrial actors (Cellnex, Everis, GMV, AIA, GTD, Keysight, KPMG, Qilimanjaro, Quside, Sateliot, Zymvol, LuxQuanta and Secpho cluster, etc.) that have come together to promote quantum tech transfer projects and innovation with a short-term or mid-term industrial and social impact.

Catalonia Quantum Academy: The Catalonia Quantum Academy will help attract & train the next generation of quantum scientists and engineers, strengthening the region's capacity to develop and deploy current & future quantum technologies.

Qollserola – Quantum ring of Barcelona: This quantum communications ring will be established in close collaboration and connection with other national and international initiatives, in the EuroQCI. Ultimately, the ring will connect different entities, companies, universities, hospitals and public administrations, paving the way for future connections via land or satellite with other metropolitan nodes in Catalonia, Spain and the EU.

Among **EuroQCI@Cat**: Terrestrial and free-space quantum links, as well as academic and industrial use cases and planning of a new OGS (Optical Ground Station).

Generalitat de Catalunya
Departament de la Presidència
Secretaria de Telecomunicacions i Transformació Digital

From Optical Fibre Network to Quantum Network

Design and tendering for a public quantum network

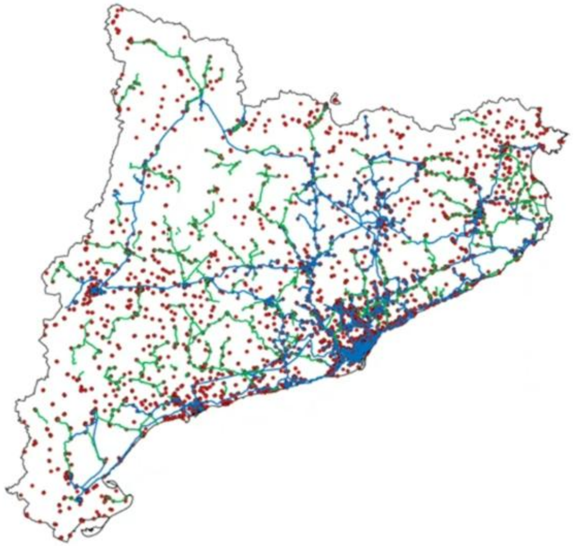
Current network architecture

Public Ownership Network of Catalonia

More than 8.000km and still deploying. Backbone done, main cities connected, right now arriving to small cities (more than 500 inhabitants).

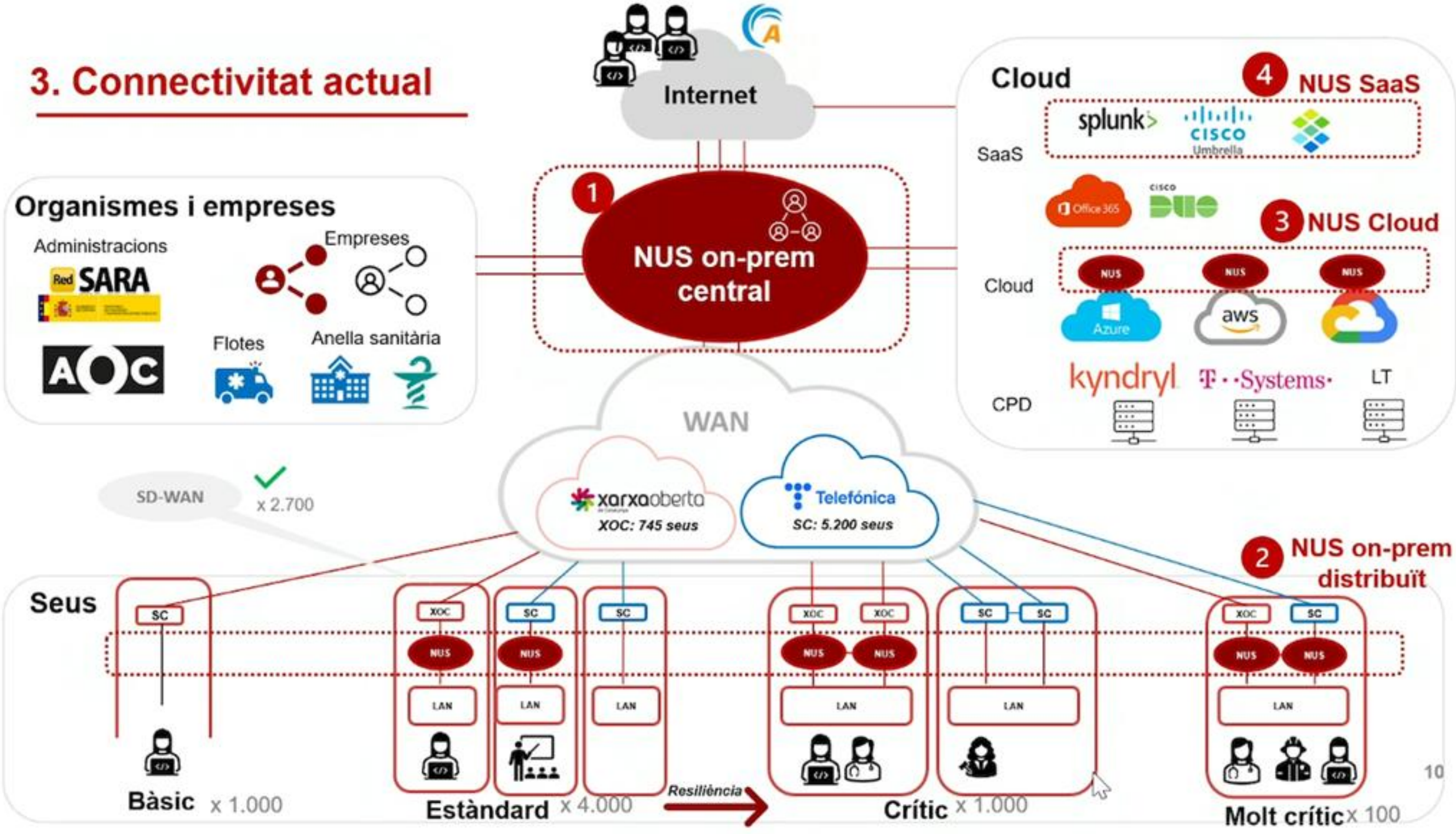
Conducts, optical fibre, underground. Point of presence on small villages. Doesn't offer services to citizens or companies, just to Regional Government sites. Wholesale services for operators (ducts, dark fibre, active services).

Providing services to Regional Government (including healthcare, police, justice, education –including universities-, offices, etc).



Locations	>6.000
Km	>8.000Km
Backbone	Different rings
Optical Fibre	Underground o.f. (not aerial)
Services	Cloud (public/private, SaaS)
Datacentres	2 on premises

Network: Logic diagram



Preparing the migration (to consider in Migration Plan)

System requirements

Scenario to consider (links length, actual system equipment, etc.)

Criteria for migrating nodes to QKD nodes

- Prioritization (exclusionary criteria at initial migration)
- Prioritization (criticality and safety)

Calculate demand for QKD keys

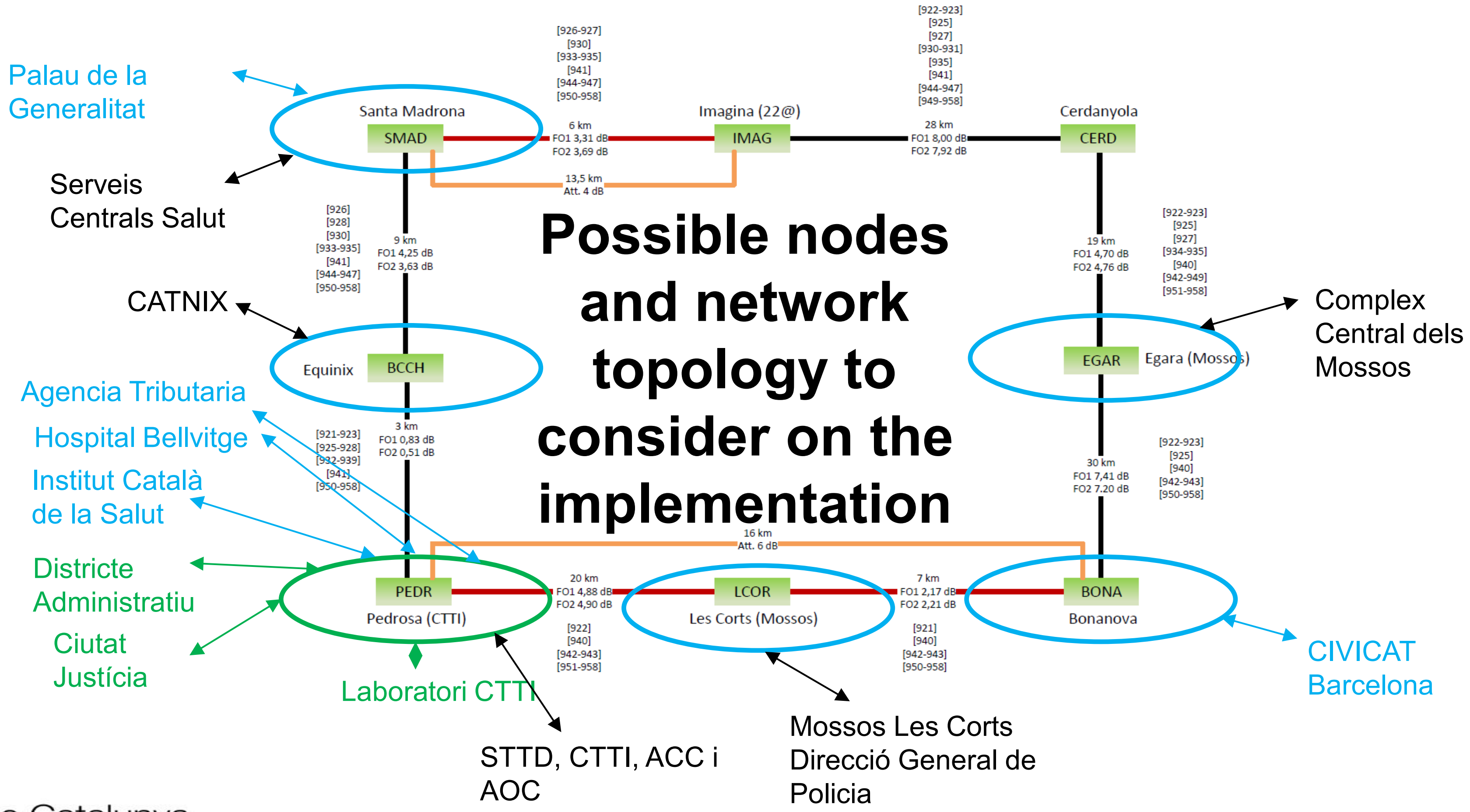
Power budget (dB)

Key generation rate

Other considerations:

- Cryptographic hybridization (PQC & QKD)
- Co-propagation (with classical traffic in the C-band)
- Integrate P2MP configuration
- Interchangeable units (not paired from the factory)
- Compact size
- Interoperability (ETSI GS QKD 004 and ETSI GS QKD 014, standards from key delivery classic and quantum)

Scenario to consider



Possible nodes and network topology to consider on the implementation

Palau de la Generalitat

Serveis Centrals Salut

CATNIX

Agencia Tributaria

Hospital Bellvitge

Institut Català de la Salut

Districte Administratiu

Ciutat Justícia

Laboratori CTTI

STTD, CTTI, ACC i AOC

Mossos Les Corts Direcció General de Policia

Complex Central dels Mossos

CIVICAT Barcelona

Criteria for migrating nodes to QKD nodes (1/4)

Prioritization (exclusionary criteria at initial migration)

1. Infrastructure availability:
   1. Availability of existing optical nodes.
   2. Availability of existing fiber links.

2. Technical feasibility to implement QKD:
   1. Admissible distances and link losses depending on the type and characteristics of the QKD devices considered.
   2. Availability of capacity at the nodes for the deployment of the equipment required for the QKD network (available rack space, required power of the electrical network, etc.).

Criteria for migrating nodes to QKD nodes (2/4)

Prioritization (criticality and safety)

3. Criticality of the entities supported by the network, considering the following as priorities:
    1. Institutions of the Regional Government (Parliament, Presidency and Government)
    2. Department of the Interior and Public Security
    3. Department of Economy and Finance
    4. Department of Health
    5. Department of Justice and Democratic Quality
    6. CTTI Network as critical infrastructure (CTTI is the public company which manages all ICT infrastructures and services for the Regional Government, Generalitat de Catalunya)
4. Criticality by business criteria
    1. Most critical sites (100)
    2. Critical sites (1000)
    3. Standard / Basic sites (4000 /1000)

Criteria for migrating nodes to QKD nodes (3/4)

Prioritization (criticality and safety)

5. Cybersecurity criteria:
   1. According to the categorization of risks in the Generalitat resulting from the threat model and profiling
   2. Frequency of cyberattacks registered in the different services and their severity
   3. Degree of security required according to the service, applying the most optimal solution (classic, PQC, QKD, hybrid)
6. Criticality by volume of information:
   1. Nodes with the highest volume of information (number of existing fiber links with other optical nodes also existing)
   2. Number of headquarters per area that depend on a node
7. Network topology:
   1. Location of the nodes in the network topology, to favor an initial compact QKD network deployment and avoiding the presence of isolated nodes or subnetworks

Criteria for migrating nodes to QKD nodes (4/4)

Prioritization (criticality and safety)

8. Connectivity to the European Quantum Communications Infrastructure (EuroQCI)
9. Technical feasibility to implement QKD (not exclusive):
    1. Availability in the nodes of encryption equipment that supports standard QKD key consumption APIs, natively or through firmware update
10. Economic conditions of deployment:
    1. Cost for deployment of non-existing (but planned) nodes
    2. Cost for deployment of non-existing (but planned) fiber optic links
    3. Cost for including QKD devices in non-existing (but planned) intermediate nodes

Calculate demand for QKD keys

Make hypothesis, calculate and consider a reasonable ratio

To analyze the volume of QKD keys that will be consumed to protect the communications network, a scenario is considered where these QKD keys are not used directly to protect these communications, but are used as a seed (K_{seed}) for a KDF (Key Derivation Function) function that generates the communications protection keys K_c.

Considering a policy of renewing the K_{seed} every 100 Kbits of generated communication key K_c, can select nodes without acceptable key rate (>100 Kbits), they are considered out of policy.

And considering a 1Gbit/second communications service and a policy of renewing a K_c key for each Gbit, the scenario is placed in the “1 second” column, where the first admissible values of Kseed renewal are for every 25 or 2.5 Kbits of generated K_c, requiring a new QKD key at least every 100 or 10 seconds for a single communication encryption service (QKD devices in a node will support a multitude of services).

Cripto Period K_{seed}	Cripto Period K_c (seconds)							Kbits
Seconds	0,001	0,01	0,1	1	10	100	1000	
0,01	2,5	0,3	0,0250	0,0025	0,0003	0,000025	0,000003	
0,10	25,0	2,5	0,3	0,03	0,003	0,000	0,0000	
1,00	250,0	25,0	2,5	0,3	0,03	0,003	0,0003	
10,00	2.500,0	250,0	25,0	2,5	0,3	0,03	0,0025	
100,00	25.000,0	2.500,0	250,0	25,0	2,5	0,3	0,025	
1.000,00	250.000,0	25.000,0	2.500,0	250,0	25,0	2,5	0,3	
10.000,00	2.500.000,0	250.000,0	25.000,0	2.500,0	250,0	25,0	2,5	
100.000,00	25.000.000,0	2.500.000,0	250.000,0	25.000,0	2.500,0	250,0	25,0	

POWER BUDGET (dB)

Depending on distance and elements on the link

A power budget (maximum tolerable losses by the system) of 18 dB or more is recommended for deployed QKD systems to cover the typical maximum distances of a metropolitan network. Although links may have lower losses (e.g., < 8 dB), this value of 18 dB will allow flexibility to support changes in the infrastructure or possible increases in losses due to other network components.

Optical networks are composed of multiple elements such as multiplexers, connectors and splices, which introduces additional losses to the system along the optical link. Mainly in the case of WDM networks, although the distances may be short, additional losses are expected if there are additional network components in the link, for example, ROADM losses are usually between 3 and 6 dB.

KEY GENERATION RATE

Necessary key generation rate for our system

The analysis presented establishes that the KMS can request QKD keys at least every 10 seconds for a single service. Considering 256 key bits, this would represent a key generation rate of around 25 bits per second per service.

Given that multiple applications and services could be established, a minimum key generation rate of 500 bits/s for the maximum distance of the systems is reasonable. Since, in the general case of QKD, the key generation rate decreases with distance and considering the links in the project with losses less than 8 dB, **a QKD system that generates keys greater than 20 kbps under these loss conditions could be considered**, which would provide flexibility for generating keys temporarily (for example during maintenance or reconfiguration).

Other considerations (1/2)

CRYPTOGRAPHIC HYBRIDIZATION

The network key manager must have the capacity to generate and distribute keys of different cryptographic nature (classical, PQC and QKD), as well as offer mechanisms for hybridizing these technologies according to the defined security policy and in accordance with the cybersecurity strategy of the Generalitat.

CO-PROPAGATION

It is recommended that QKD systems deployed in metropolitan networks allow compatibility with DWDM wavelength division multiplexing networks for co-propagation with classical traffic in the C-band (1530 nm to 1565 nm).

This allows optimizing network resources, facilitating efficient integration without the need for dedicated optical fiber. It is also recommended that the wavelength of the quantum channel of the QKD system can be customized within different values in the C-band, which will allow direct use of available DWDM channels that are not being used, minimizing the impact on the network during the deployment of QKD.

Considering the power conditions in metropolitan networks of classical channels, QKD systems should tolerate more than 5 dBm of total injected power from adjacent classical channels.

Other considerations (2/2)

MULTI-RECEIVER OR POINT-TO-MULTIPOINT (P2MP) CONFIGURATION

INTERCHANGEABLE UNITS

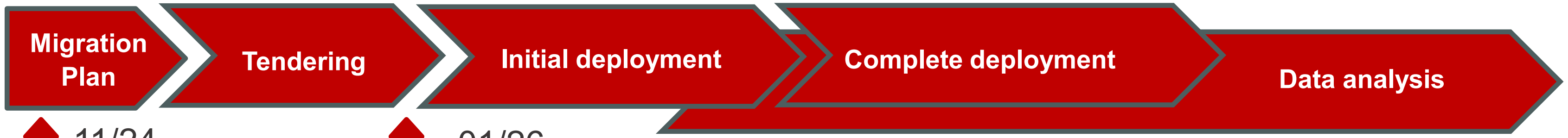
It is recommended that QKD systems deployed in metropolitan networks use interchangeable units, that is, that transmitters and receivers do not come paired from the factory.

COMPACT SIZE

INTEROPERABILITY

Finally, it is important that QKD systems comply with international standards for key delivery: **ETSI GS QKD 004** and **ETSI GS QKD 014**, so that they can be directly compatible with KMS systems and ciphers. It is also important that they have management interfaces typically used in networks, such as SNMP or HTTP interfaces.

Time plan in execution



Migration Plan

Tendering

Initial deployment

Complete deployment

Data analysis

◆ 11/24

- Node Categorization
- Node Location
- Prioritization
- Technical and Space Requirements
- Conclusions

◆ 03/25

- Drafting of specifications
- Tendering
- Receipt of offers
- Evaluation of offers
- Award

EUROPEAN UNION
European Regional Development Fund
ERDF

◆ 01/26

- Provisioning 4 initial equipment
- Test installation (lab)
- Configuration and initial test
- Network calibration

◆ 06/26

- Deployment at the 4 initial nodes of the metropolitan ring

◆ <12/26

- Provisioning 8 remaining nodes

◆ 01/27

Expansion of the deployment to 4 final nodes of the metropolitan ring

Final scaling to 6 corporate headquarters

Final: 06/27

Transversal tasks

◆ 12/27

Data analysis in the lab

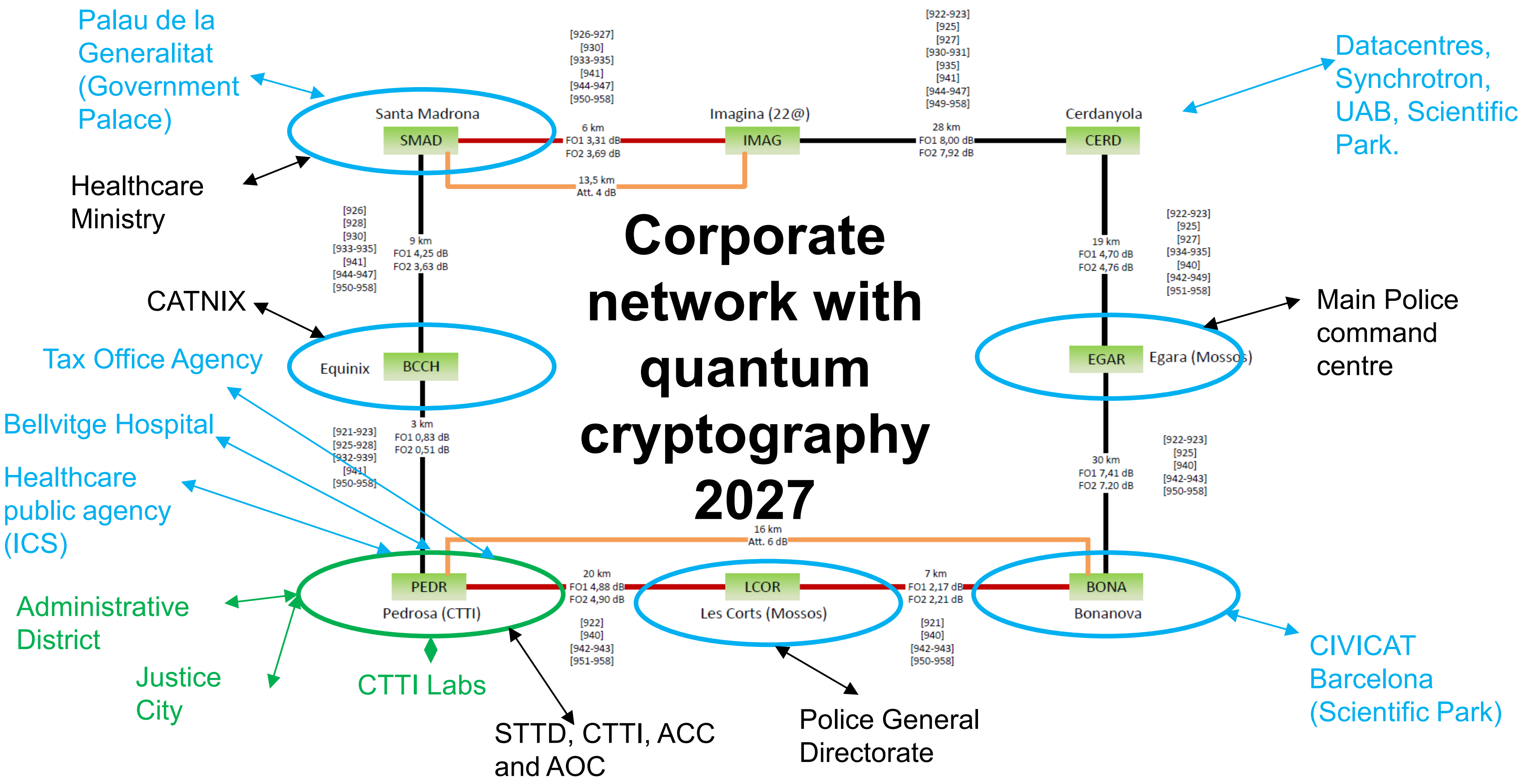
Data analysis among the first 4 headquarters of the metropolitan ring

Data analysis among the 8 headquarters of the metropolitan ring

Data analysis with the 6 corporate headquarters, complete network

Conclusions

Quantum Network 2027: Logic topology



Palau de la Generalitat (Government Palace)

Healthcare Ministry

CATNIX

Tax Office Agency

Bellvitge Hospital

Healthcare public agency (ICS)

Administrative District

Justice City

CTTI Labs

STTD, CTTI, ACC and AOC

Police General Directorate

CIVICAT Barcelona (Scientific Park)

Main Police command centre

Datacentres, Synchrotron, UAB, Scientific Park.

Corporate network with quantum cryptography 2027

Santa Madrona
SMAD

Imagina (22@)
IMAG

Cerdanyola
CERD

Equinix
BCCH

EGAR
Egara (Mossos)

PEDR
Pedrosa (CTTI)

LCOR
Les Corts (Mossos)

BONA
Bonanova

[926-927]
[930]
[933-935]
[941]
[944-947]
[950-958]

6 km
FO1 3,31 dB
FO2 3,69 dB

13,5 km
Att. 4 dB

[922-923]
[925]
[927]
[930-931]
[935]
[941]
[944-947]
[949-958]

28 km
FO1 8,00 dB
FO2 7,92 dB

[926]
[928]
[930]
[933-935]
[941]
[944-947]
[950-958]

9 km
FO1 4,25 dB
FO2 3,63 dB

19 km
FO1 4,70 dB
FO2 4,76 dB

[922-923]
[925]
[927]
[934-935]
[940]
[942-949]
[951-958]

[921-923]
[925-928]
[932-939]
[941]
[950-958]

3 km
FO1 0,83 dB
FO2 0,51 dB

30 km
FO1 7,41 dB
FO2 7.20 dB

[922-923]
[925]
[940]
[942-943]
[950-958]

16 km
Att. 6 dB

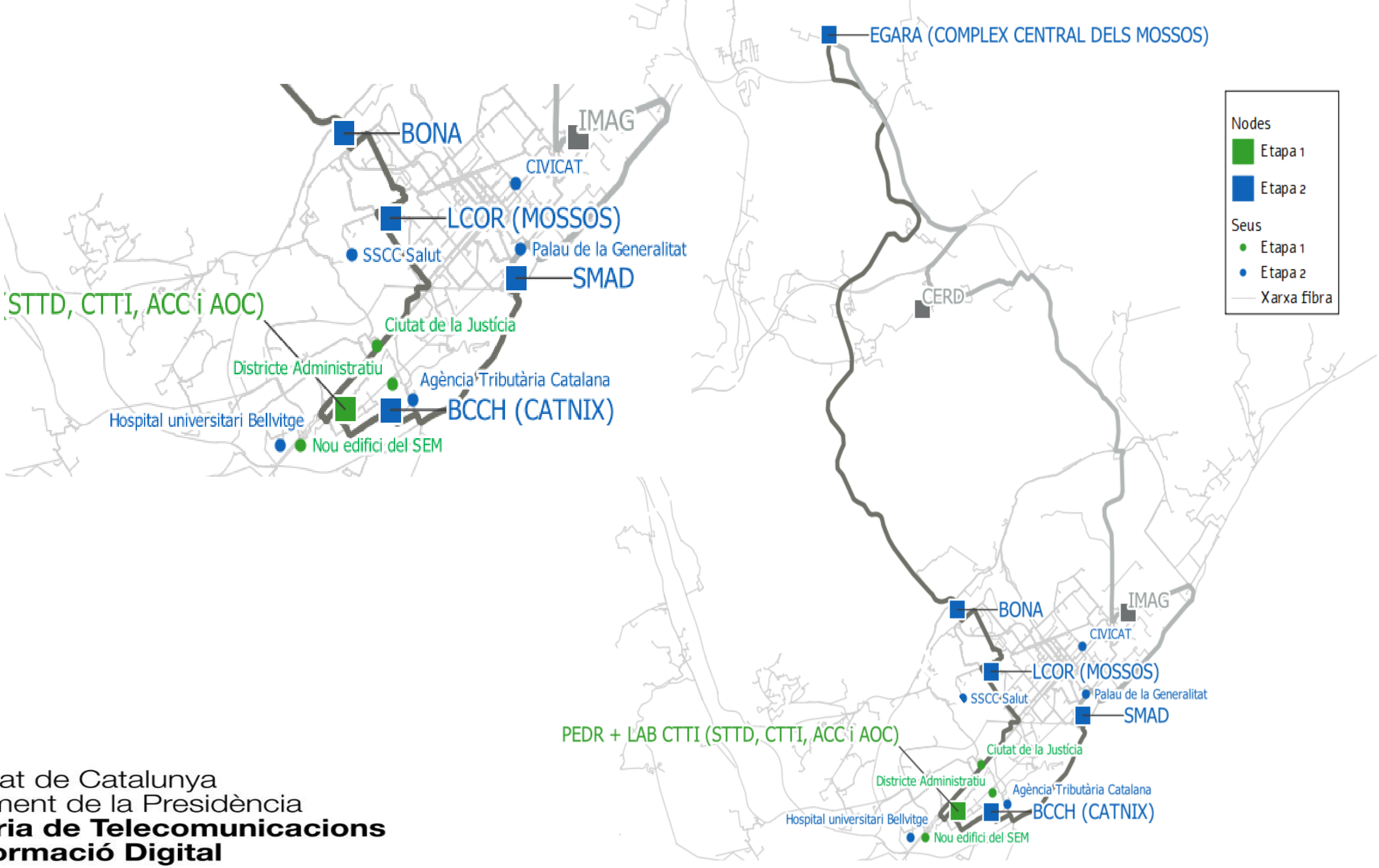
20 km
FO1 4,88 dB
FO2 4,90 dB

[922]
[940]
[942-943]
[951-958]

7 km
FO1 2,17 dB
FO2 2,21 dB

[921]
[940]
[942-943]
[950-958]

Corporate network with quantum cryptography 2027



Phase 0 (11/24 – 03/25)

This initial phase covers the deployment of 5 QKD-KMS systems in pre-production. The objective is to integrate and validate the interconnection of all the necessary equipment in a laboratory environment, to raise the maturity of the technology to a TRL8. This was achieved by carrying out the first tests and commissioning of the technology, ensuring interoperability for its subsequent deployment to the nodes in production.

During this phase, it is essential that the KMS, QKD and Generalitat manufacturers collaborate closely to ensure that the comprehensive solution meets all the requirements identified for deployment in production environments. This stage will allow the **use cases, applications and services** available to be precisely defined, as well as essential operational aspects, such as integrated management and monitoring of the solution.

In addition, it is convenient to start the analysis of the points collected in Phase 1 to begin the development of the threat model and profiling. The results of these analyses will be necessary to address prioritization criteria #5 that respond to the needs in terms of cybersecurity of the Generalitat's services.

Phase 1 (03/25 – 01/26)

This phase is divided into **two stages**. The first stage covers the transfer of pre-production QKD capabilities to **4 nodes of the network in production**, **maintaining 1 in pre-production**. This stage will allow validating the technology in a real environment, providing QKD keys to priority services of the Generalitat (Regional Government). Once this stage is completed, the second stage would begin, where the objective is to extend the deployment to cover a total of **14 nodes** of the network.

For the selection of the nodes, a list of possible nodes was analyzed, and these are a total of 76 starting nodes, and the criteria identified in previous sections. First, by applying the exclusion criterion 1 – “Availability of infrastructure”, the initial list is reduced to 27 nodes.

Next, we assign the following weights to each criterion, so that the maximum score a node can achieve is 1.

So, we conclude with a new table including the final score received by the 27 nodes, not excluded by criterion #1 and we select the nodes shown on the Quantum Network 2027 in previous slides.

Analysis and next phases

Phase 2 (till end 2027)

- Data analysis in the lab
- Data analysis among the first 4 headquarters of the metropolitan ring
- Data analysis among the 8 headquarters of the metropolitan ring
- Data analysis with the 6 corporate headquarters, complete network
- Conclusions

Possible next phases

Complete with pending nodes to accomplish criteria “Network Topology”. Create complete rings and validate performance in different network topologies (create rings into rings, different traffics, manage different network topologies, etc.).

Generalitat de Catalunya
Departament de la Presidència
**Secretaria de Telecomunicacions
i Transformació Digital**

gencat.cat