EU Quantum Technologies Flagship and the quantum internet

ENISA TELECOM SECURITY FORUM

29 June 2022

Jean-François Buggenhout
Head of Unit DG CNECT.C4
Emerging & Disruptive Technologies

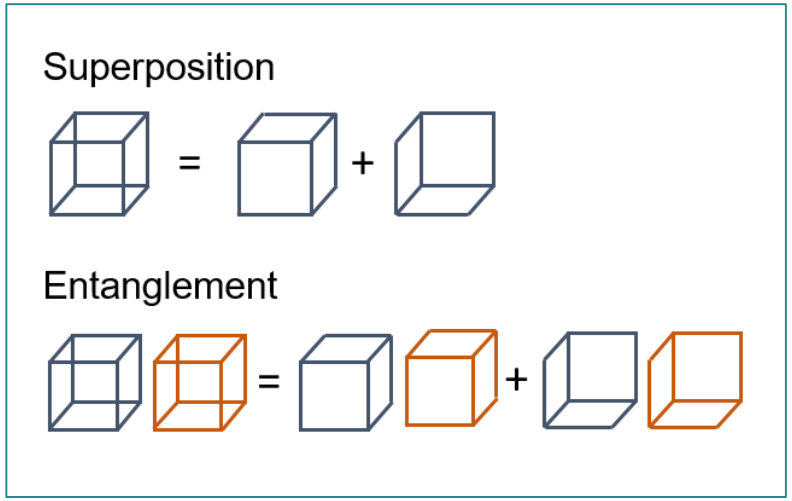
Quantum Technologies (QT)

- Quantum mechanics describes the “ultrasmall” – single particles (electrons, atoms, ions) and indivisible units of light and radiation (photons).
- Quantum technologies make use of the properties of quantum mechanics

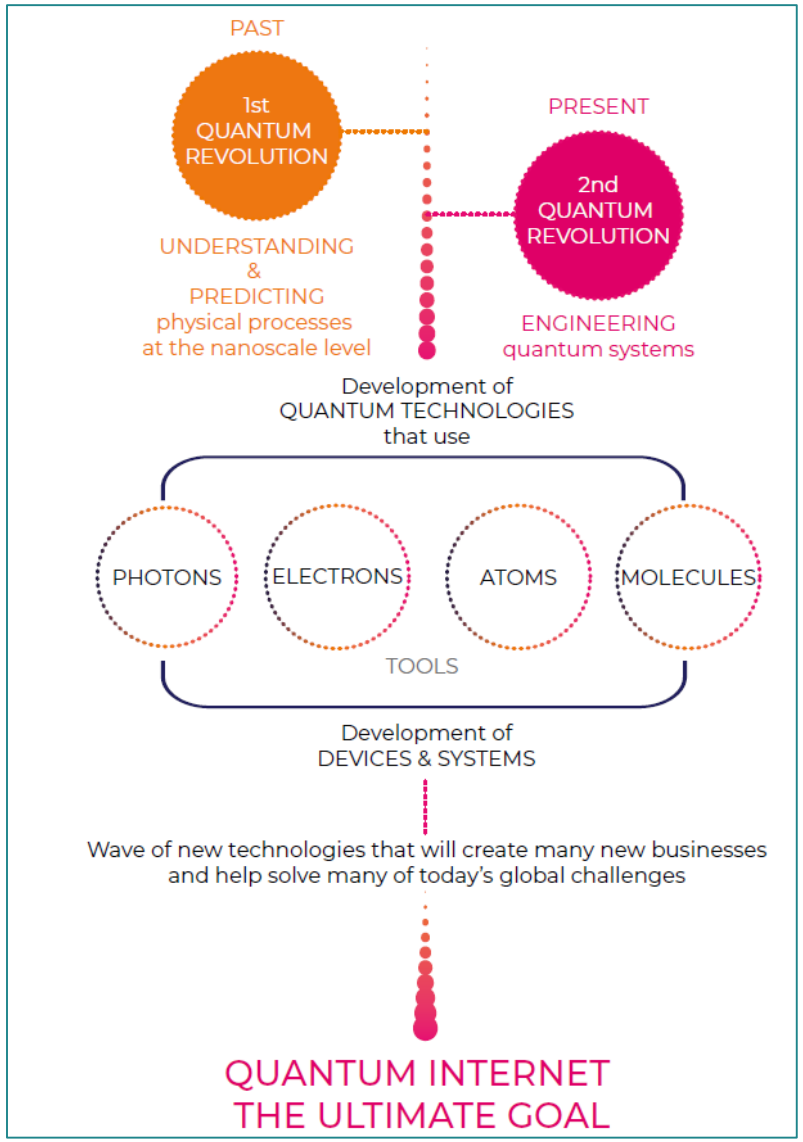
“things can be in more than one state at the same time”

“observation (measurement) changes the observed object”

“the state of two distant objects can be linked”



The second quantum revolution



The second quantum revolution is all about controlling individual quantum systems, such as charged molecules, to a greater extent than before, enabling even more powerful applications of quantum information. *(NIST)*

EU has scientific leadership in QT

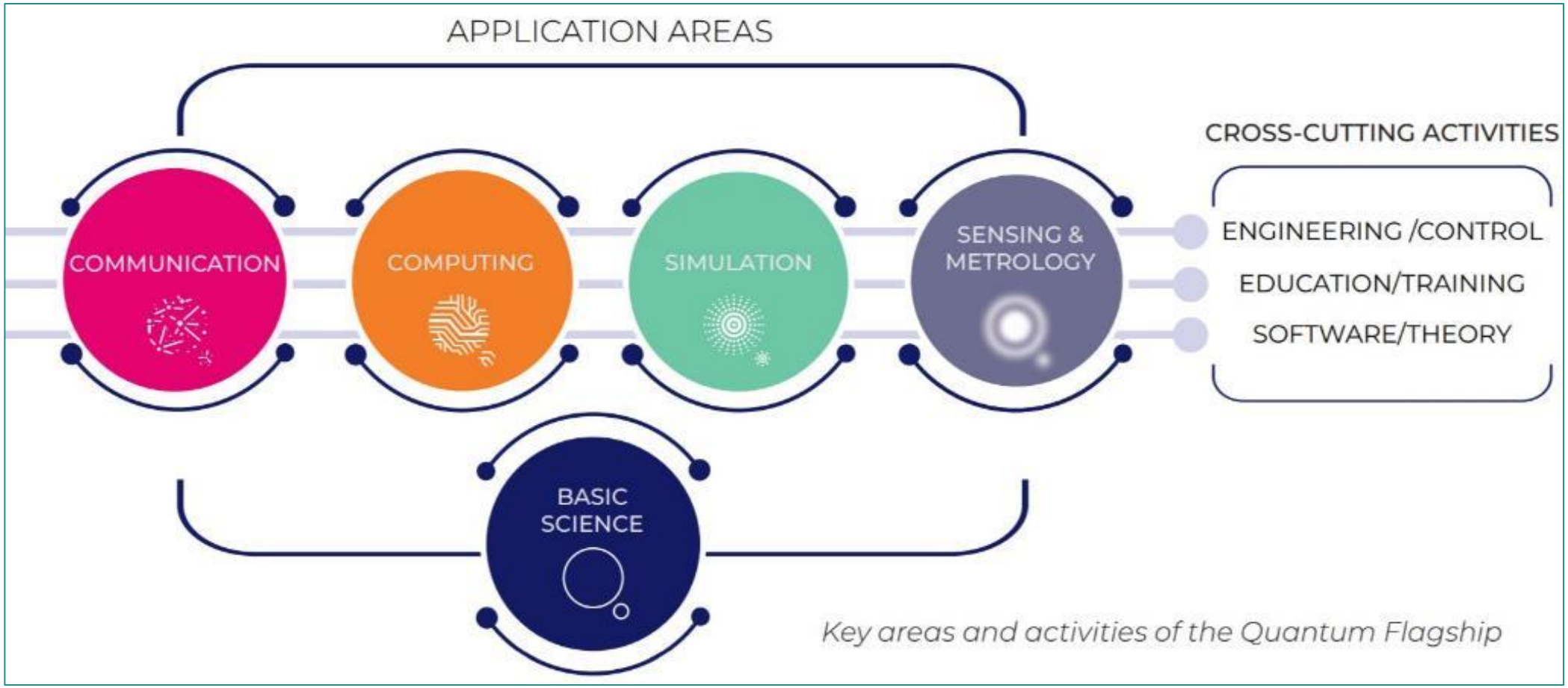
Alain Aspect
(EPR paradox - 1980)

Serge Haroche
Nobel in Physics 2012

…and aims at industrial leadership

European Commission

The Quantum Technologies Flagship



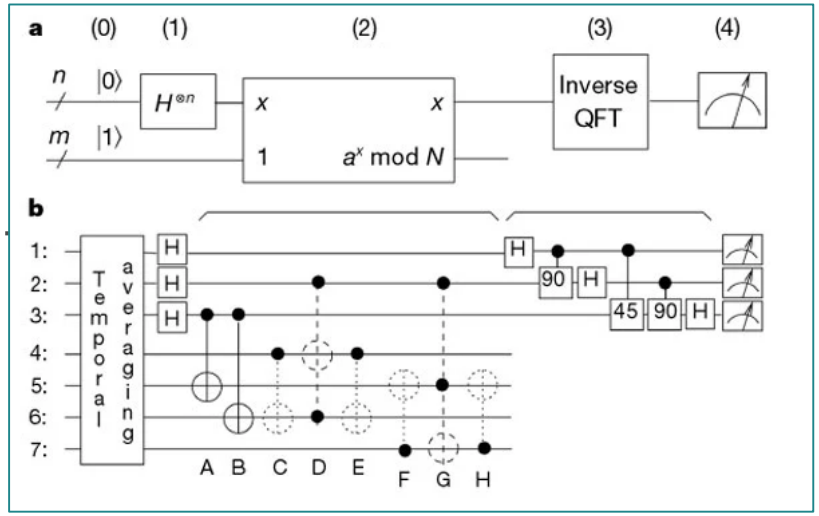
Key areas and activities of the Quantum Flagship

Quantum technologies & cybersecurity

- Quantum random number generators: source of true randomness
- Quantum computing: harnessing the collective properties of quantum states (superposition, interference, entanglement)
- Quantum sensors: detect the variation of physical properties at atomic level
- Quantum communication: uses quantum properties to securely exchange information

The threat of quantum computers

- Cryptography relies on mathematical complexity
- Quantum computers bring radically new computing
- New quantum algorithms emerge and will continue
- Threat on robustness of existing algorithms



https://www.nature.com/articles/414883a

"A cryptographically relevant Quantum Computer will be available by the beginning of the 2030ies." (BSI)

"Quantum Computing is for tomorrow, but Quantum-related risk is here today" (Security Week, Jan 2022)

European Commission

Addressing the QC threat

- Post-quantum cryptography
  - New crypto algorithms that are believed to resist to the increase of computing power and specific properties of quantum computers
- Quantum key distribution
  - Exchange an initial secret, encoded on quantum states (usually photons)
  - Use it to encrypt communications the standard way

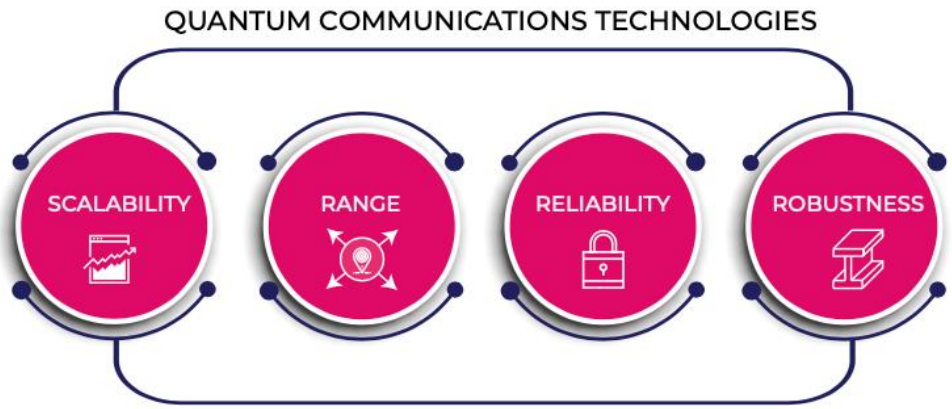
Don’t bet on a single horse.

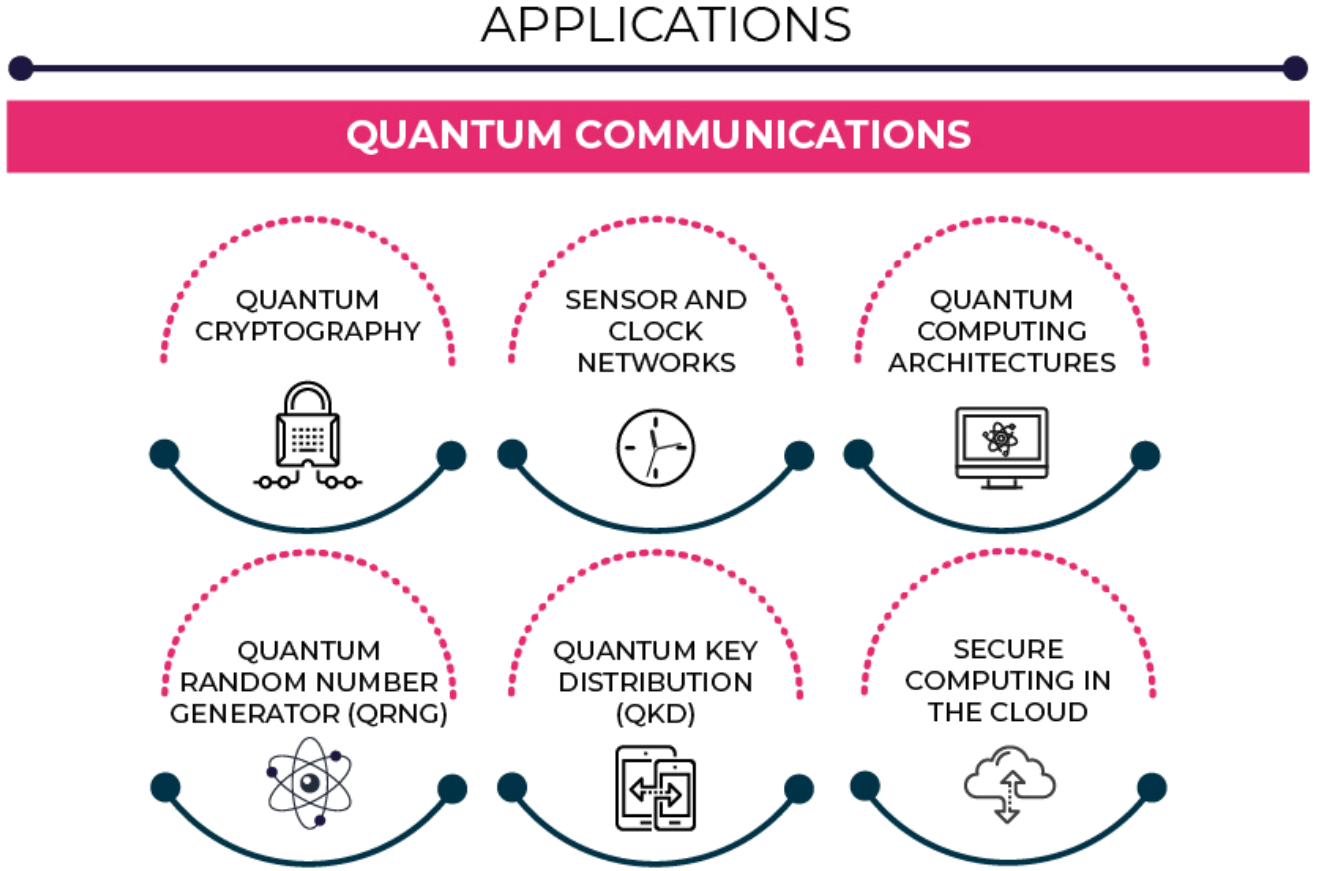
Post-quantum cryptography and Quantum Communication will complement each other.

Quantum Communication: the Flagship's goals

QUANTUM FLAGSHIP

Quantum communication will build on the current digital infrastructure to distribute and connect quantum resources for improved security and functionality. This will address challenges such as the long-term security of health records, to connected quantum clock networks and eventually enabling secure connection to quantum computers in the cloud.





European Commission

EuroQCI:
A pan-EU quantum communication infrastructure

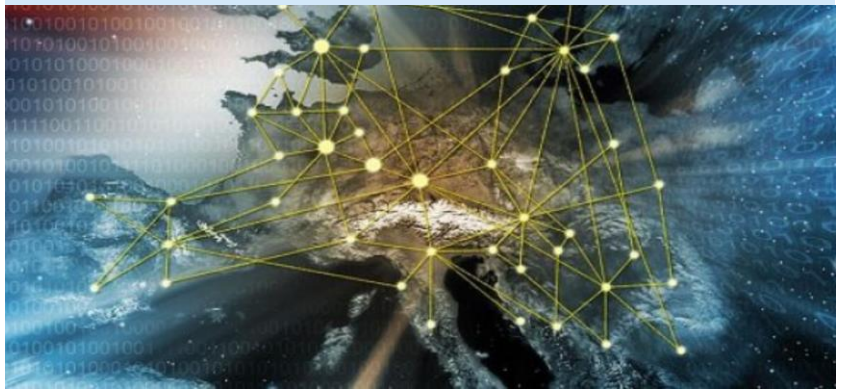
- An integrated satellite and terrestrial system spanning the whole EU for ultra-secure exchange of cryptographic keys (Quantum Key Distribution)
- Key objectives:
  - Equip the EU with a state-of-the art quantum communication capability, integrated into existing communication infrastructures, to help securing communications and critical infrastructures
  - Boost Europe's scientific and technological capabilities in cybersecurity and in quantum technologies
  - Improve Europe's digital sovereignty and industrial competitiveness

EuroQCI – policy context

- EuroQCI Declaration signed by all the 27 Member States
- EuroQCI is part of the European Cybersecurity Strategy and of the Secure Connectivity programme

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

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



European Commission

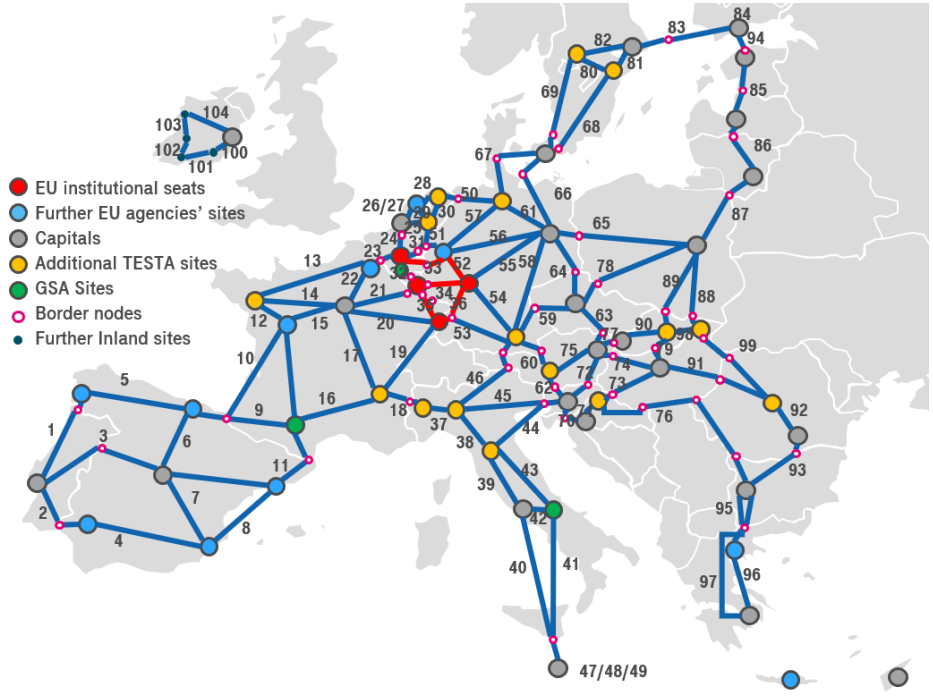
EuroQCI - key actions

- Increase EU industrial capability & mature products
- Let MS deploy their first terrestrial networks, identify use cases, test, etc
- Prepare & launch first quantum satellites
- Encourage MS to create cross-border links & link to space segment
- Work on EuroQCI specifications for next generation
- Address security aspects together with National Security Agencies
- Define and procure a testing and certification infrastructure
- Encourage EU participation in standardisation activities

EuroQCI: Terrestrial Segment

A federation of national terrestrial QCI networks

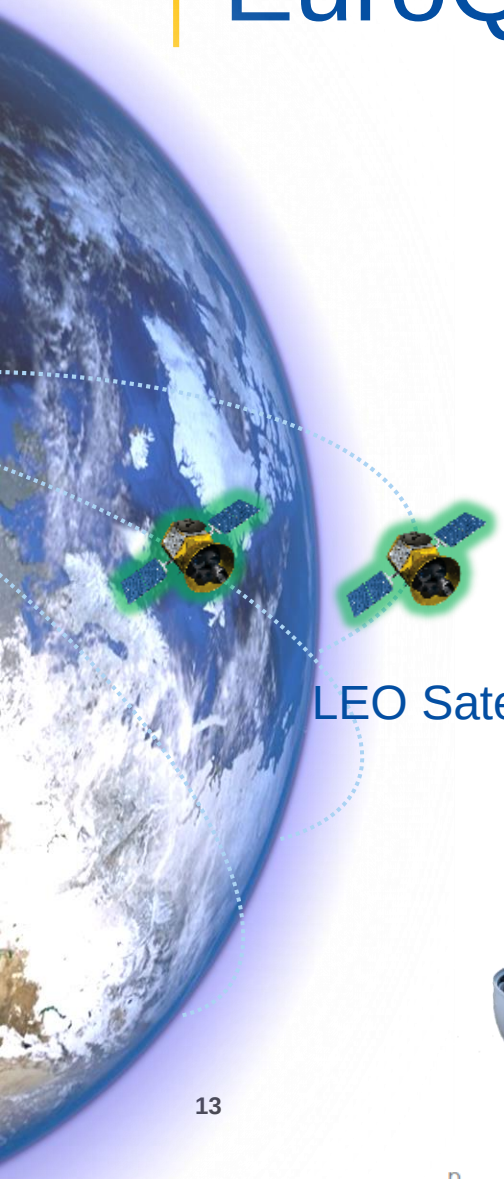
Potential sites accross the EU (study)



- Long-term vision, to be achieved incrementally by MS working on national and cross-border links over the next five years: Digital Europe Programme and Connecting Europe Facility calls ongoing
- Federation of interconnected/interoperable national networks linking key sites (governmental, critical infrastructures, etc).
- Dimensioning: fibre backbone connecting European metropolitan areas in all 27 MS + relay nodes (currently ~100 km max fibre length). Total length of about 44,000 km

European Commission

EuroQCI: Space Segment



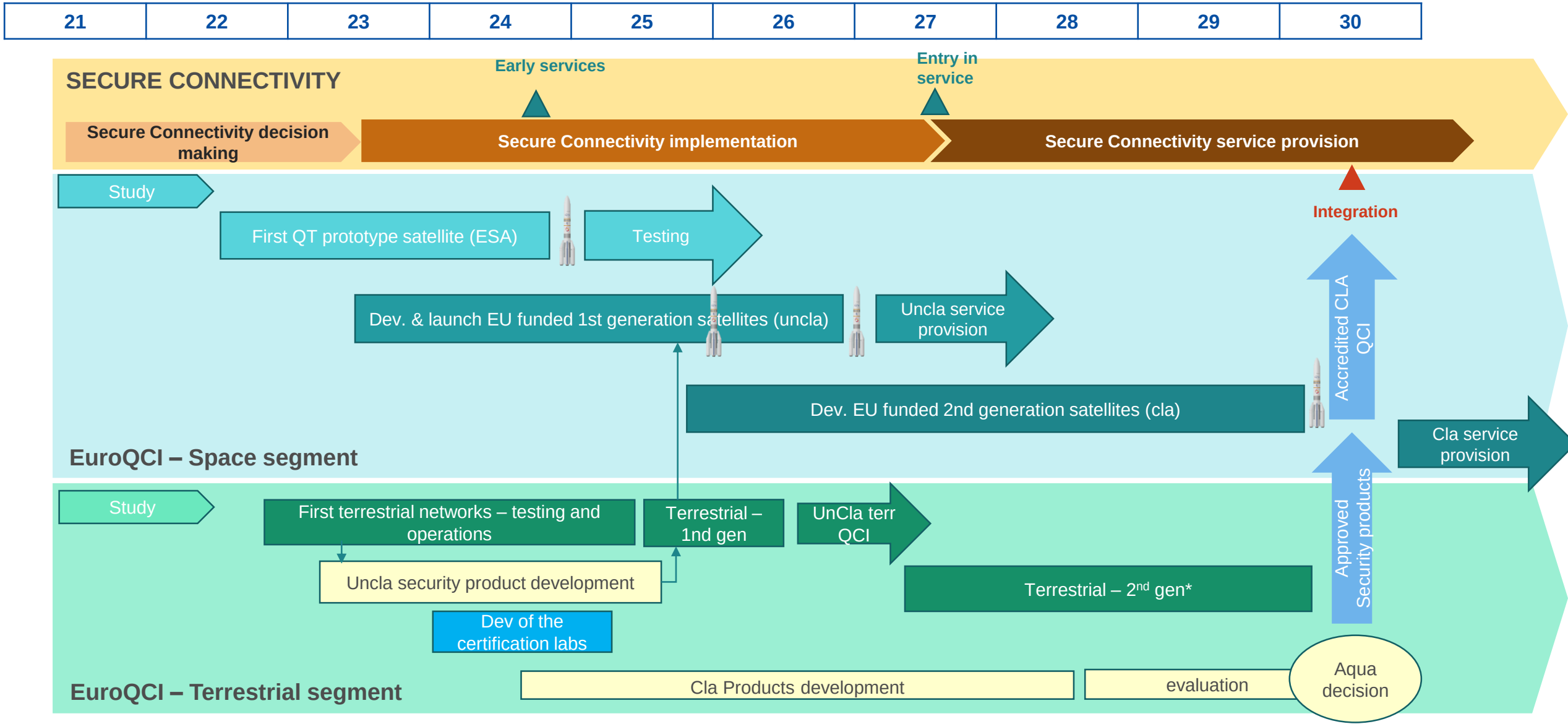
LEO Satellites

Key technologies

- End 2024: Pre-deployment of a first LEO satellite (Eagle 1) - technical proof of concept
- 2025-2026: Deployment of a 1st generation constellation LEO satellites - pre-validation: end to end QKD between different sites

13

EuroQCI & Secure Connectivity - schedule



Thank you

European Commission