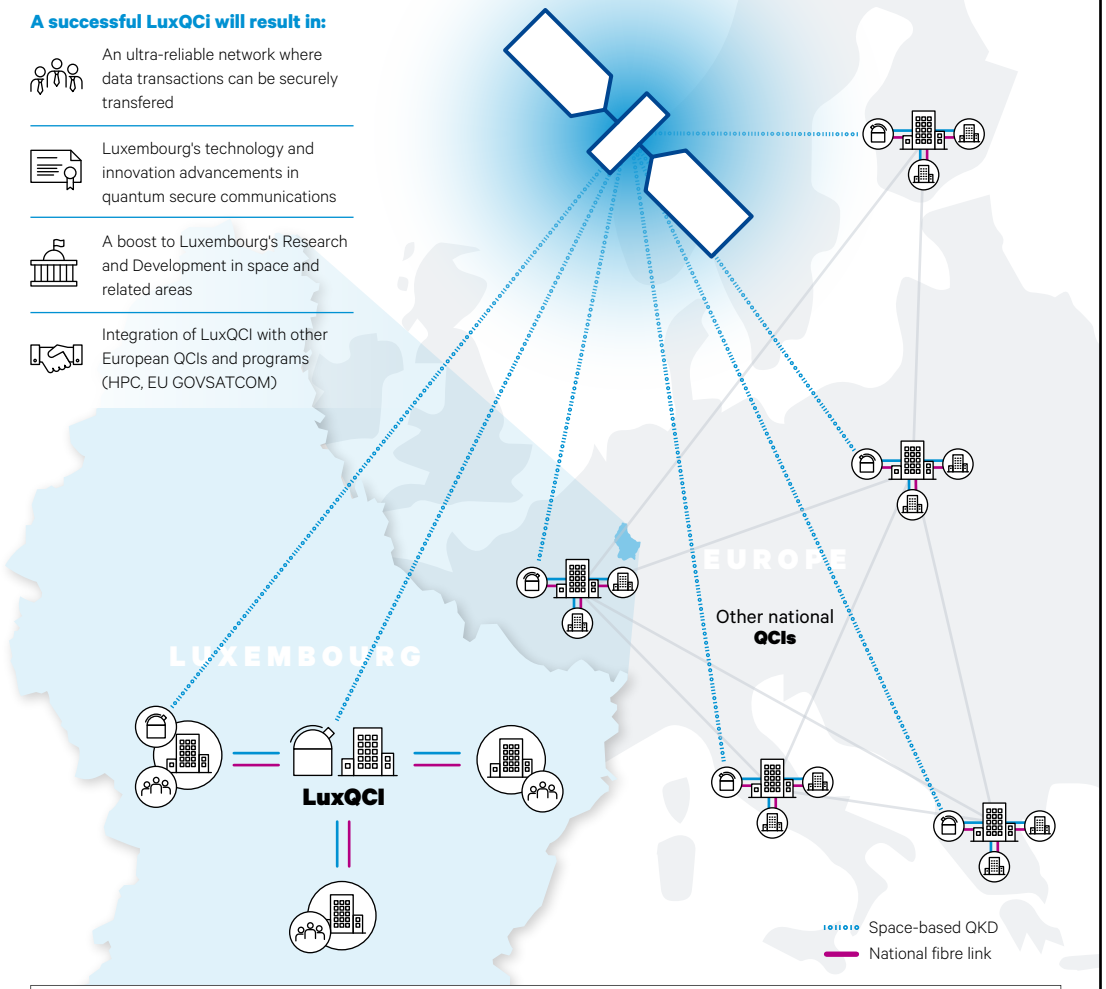
SES-LED CONSORTIUM TO BUILD LUXEMBOURG'S QUANTUM COMMUNICATION INFRASTRUCTURE

LuxQCI is a secure communication shield comprising satellite & terrestrial network for cybersecurity

A successful LuxQCi will result in:

- An ultra-reliable network where data transactions can be securely transfered
- Luxembourg's technology and innovation advancements in quantum secure communications
- A boost to Luxembourg's Research and Development in space and related areas
- Integration of LuxQCI with other European QCIs and programs (HPC, EU GOVSATCOM)



The LuxQCI project is coordinated by the Department of Media, Telecommunications and Digital Policy (SMC) of the Luxembourg Ministry of State, and is supported by the European Space Agency (ESA) and the Luxembourg Space Agency (LSA) under the Luxembourg National LuxIMPULSE programme.

Basics of quantum communications

1. Quantum Communications Infrastructure (QCI)

The aim of the QCI is to provide a quantum secure communication shield to protect the economy and society from cyber threats. Only a combination of terrestrial and space technology can guarantee security of digital transactions over short and long distances between continents. Early users include government agencies that require a high level of security to transmit confidential information. In 2019, a technical agreement signed between the European Commission and the European Space Agency laid the first stone in the creation of a pan-European quantum communication infrastructure.

2. Quantum Key Distribution (QKD)

QKD is a component of QCI that ensures ultra-secure form of cryptographic key sharing between users. It leverages the principles of quantum mechanics to provide the sender and recipient of an encrypted message with an intrinsically secure random key in geographically-dispersed areas. QKD delivered over satellite is essential to ensure long distance key distribution.

3. Quantum Computing

Radically different from classical computing based on binary bits. A quantum bit, or qubit, can be used to perform parallel computation much faster, thanks to the quantum-mechanical phenomena. Because the current public-key cryptography will inevitably be broken by ever more powerful computing, new forms of encryption that are quantum-resistant are required.

4. Quantum Internet

In the long run, Europe aims to built quantum internet by interconnecting quantum computers, simulators and sensors via quantum networks that distribute information and quantum resources.

QKD: satellite-enabled ultra-secure form of encryption