Hellas Sat

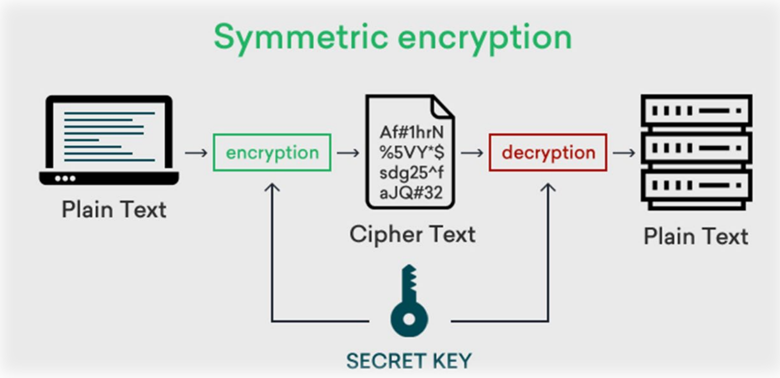
Quantum Security

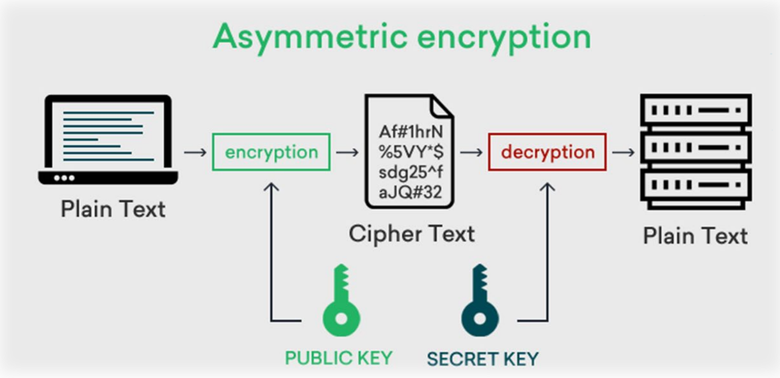
hellassat
A part of Arabsat world

Bridging worlds

Classical Cryptography

- To secure data transmission current cryptography encrypts messages using encyption **keys**
- The most secure methods today are AES-256 and RSA-4096





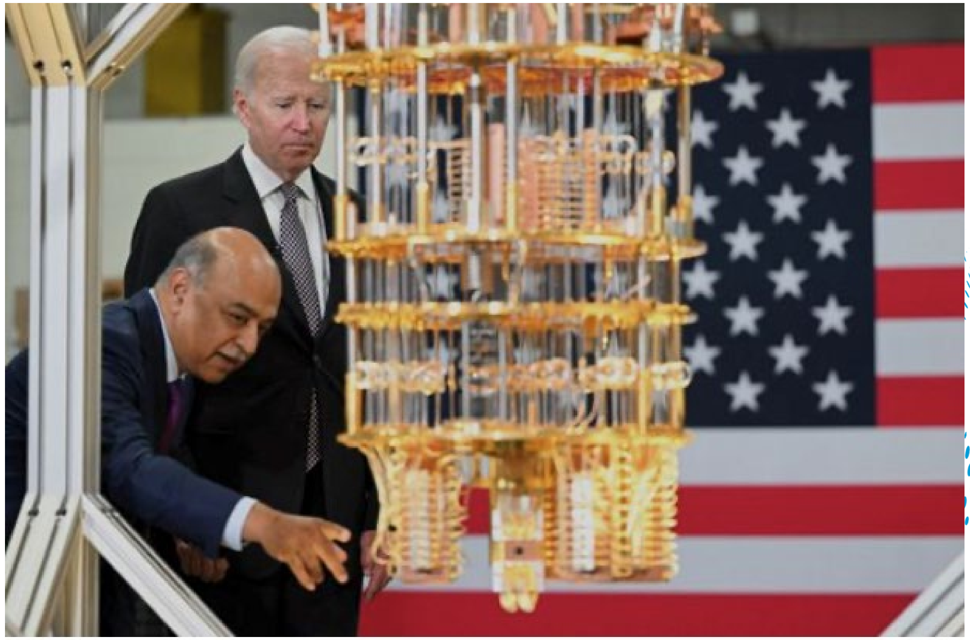
- Classical encryption relies on mathematical hardness assumptions

- The highest present cryptography standard **AES-256**, requires 2^{256} attempts to be tried requiring billions of years for any current supercomputer to break.

115,792,089,237,316,195,423,570,985,008,687,907,853,269,
984,665,640,564,039,457,584,007,913,129,639,936 ***attempts !***

The Quantum Advantage

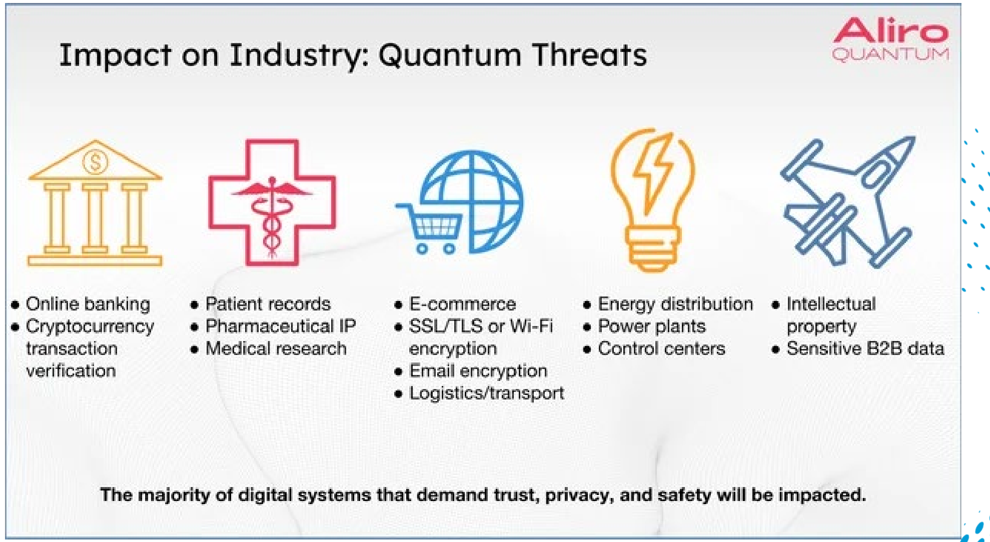
- We are currently on the edge of a quantum revolution
- Quantum Computers offer unparallel processing powers compared to classical computing
- By manipulating quantum mechanical properties, QC are able to process all possible states of a quantum bit (called qubits) at the same time.
- Google recently (July 2023) announced the execution that would take 47 years for the fastest current supercomputer (Frontier). Google QC used 70 qubits.



President Biden examining a quantum computer with IBM CEO Arvind Krishna. PHOTO: MANDEL NGAN/AGENCE FRANCE-PRESSE/GETTY IMAGES

The Quantum Threat

- Quantum Systems and hybrid Quantum-AI have the potential to compromise all current encryption systems.
- **Q-Day**: The day that large-scale quantum computers will be able to factorize the large prime numbers that unterlie our public encryption systems.
- It would take a classical computer 300 trillion years to crack an RSA 2048 bit encryption key. It would take for a QC take 10 seconds for the same task equipped with 4099 stable qubits.



Recent Advancements:

- Google and the Royal Institute of Technology (KTH) cracked a 2028-bit RSA problem in 8 hours using 20M noisy qubits compared to the theorized 1B qubits requirement speculation in 2012.
- Chinese researchers recently (2020) found methods to utilize “noisy qubits”, to solve RSA factorization problems with less coherent qubits than theoritically required (Shor algorithm).

Quantum Mechanical Properties

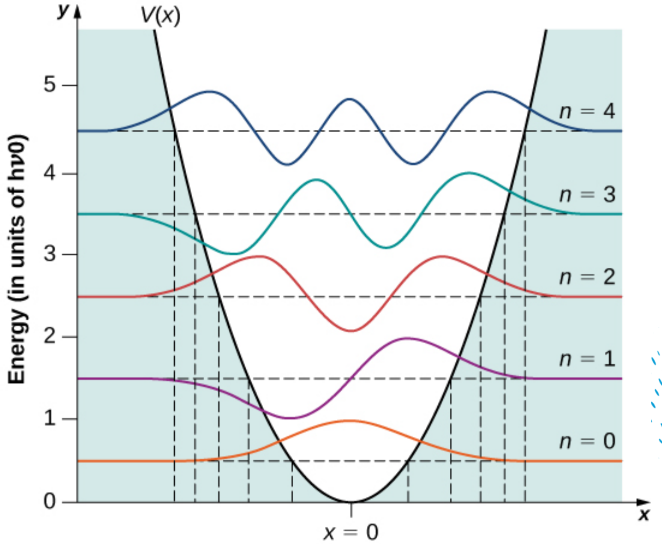
Quantum physics present non-intuitive properties:

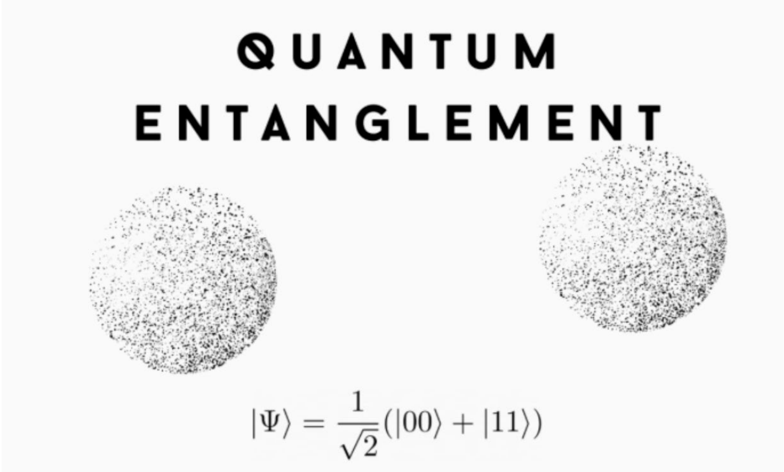
- **Superposition:** A quantum system can be in a combination of multiple states at the same time until it is measured.

- **Entanglement ("spookey action at a distance" A. Einstein):** A group of particles can be linked, so that the state of one instantaneously influences the state of the other, regardless of the distance separating them.

➢ **The above quantum-mechanical properties can be exploited to create immune encryption systems (Quantum Cryptography)**

✓ ***No Cloning Theorem: It is impossible to measure an unknown quantum state without altering its state.***

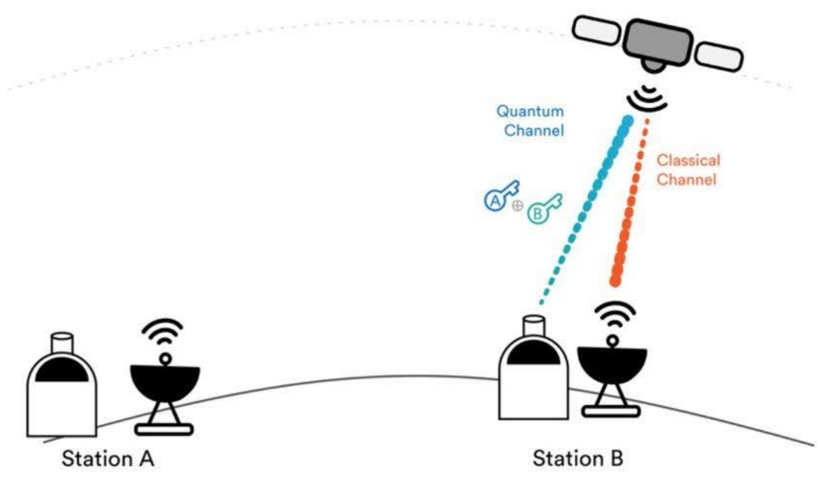




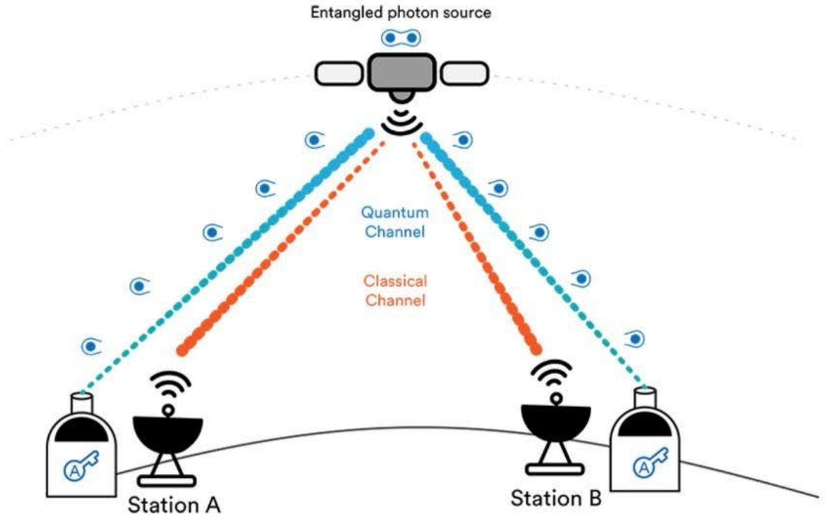
The Solution

Quantum Key Distribution (QKD)

Sequential Rendevous



Entangled Photon Source Rendevous



QKD Protocols

- **Prepare and Measure (BB84)**

  Based on a prepared encrypted key based on corellated polarization photon states (qubits) that are being read by both parties. The strength of this method is based on the no-cloning theorem.
- **Entanglment (E91)**

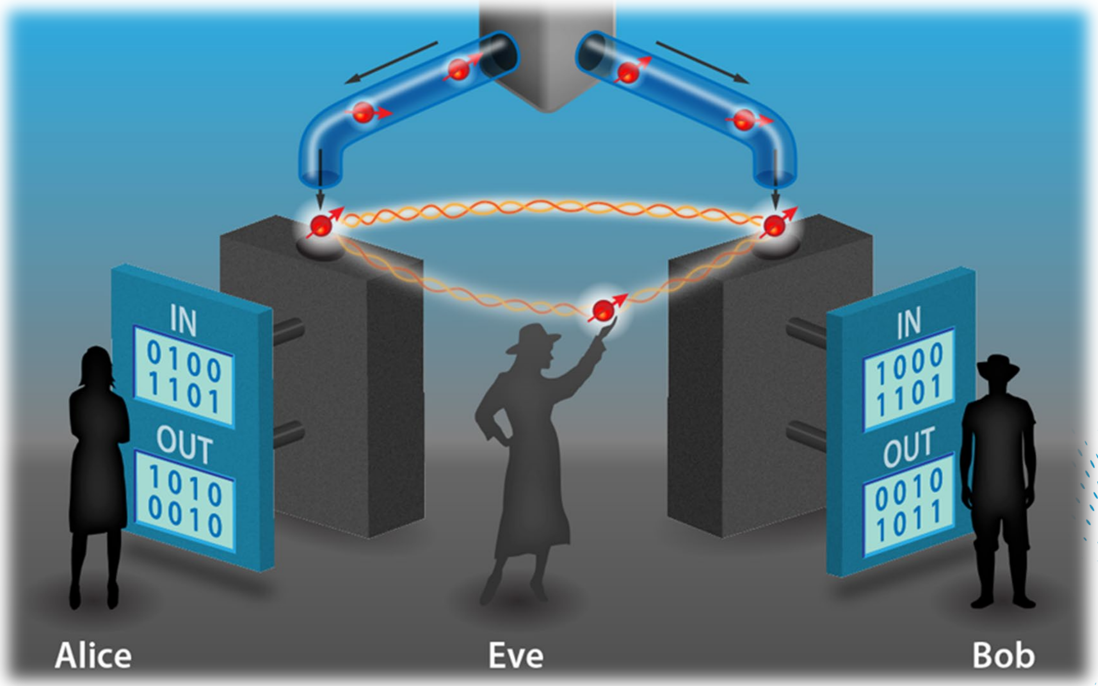
  Based on the generation of entangled photon pairs, two recipients will receive correlated results. The strength of this method is based on the absence of a random bit generator at the source.

Space QKD – Immune Encryption

For all QKD protocols, immunity to interception is warranted through two fundamental principles:

- ✓ **Quantum Properties**
  Any attempt to intercept quantum information reveals the intruder to both parties, thus the key is rejected.

- ✓ **Physical Security**
  Laser beams are extremely hard to intercept due to their narrow divergence over long distances.



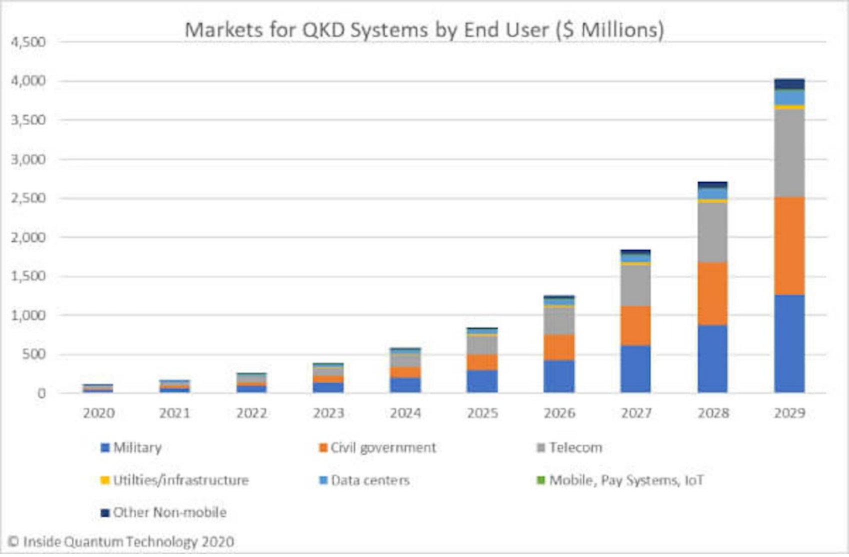
QKD Commercialization

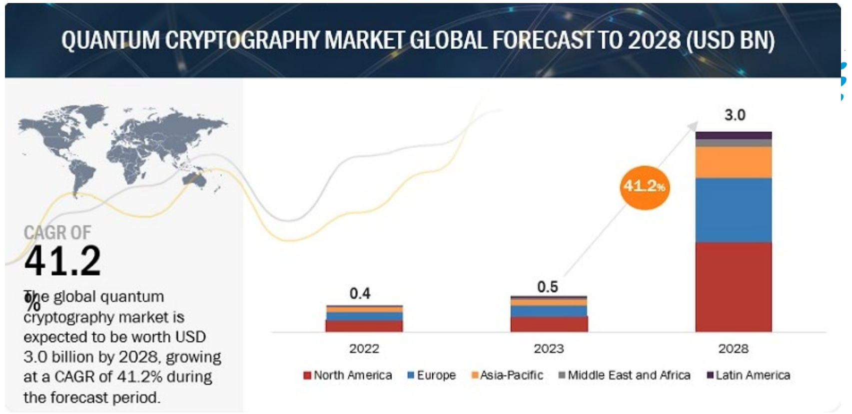
Numerous companies are currently working to commercialize QKD technology.

A non-exhaustive list:

- IDQ (Switzerland)
- QuantumCTek (China)
- CAS (China)
- Huawei (China)
- Toshiba (Japan)
- Batelle (US)
- KETS Quantum Security (Canada)
- Airbus (France)
- Photonic (Canada)
- Quantum Xchange (USA)
- IBM (US)
- QuintessenceLabs Pty (Australia)
- QuantLR
- Quantopticon
- QEYnet (Canada)
- Nu Quantum (UK)
- Qnu Labs (India)
- Qtlabs (Austria)
- Agnostiq (Canada)
- Crypto Quantique (UK)
- Infiniquant (Germany)
- ISARA (Canada)
- MagiQ Technologies (US)
- Post-Quantum (UK)
- Qasky Quantum Technology (China)

…





The Quantum Space Race

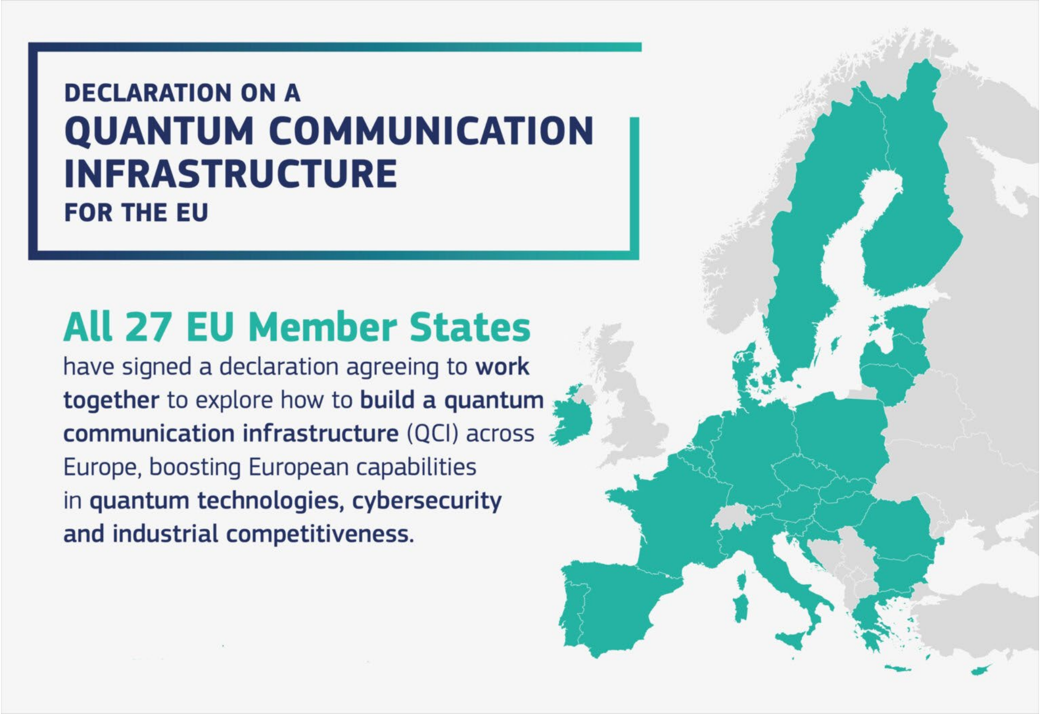
A QKD space race is under way

- China was the first to deploy a QKD satellite (**Micius**) in 2016 and demostrated quantum encrypted communications between two Beijing and Vienna.
- Jananese SOTA laser (world's smallest quantum transmitter) onboard **SOCRATES** satellite demonstrated QKD signals transmission
- **Tiangong-2 Space Lab** demonstrated space-to-ground QKD in 2017
- ESA/SES **Eagle-1** will be the first QKD satellite expected to be launched in 2024 (Sitael,Tesat) to demonstrate the European Comission's EuroQSI program.
- **SpeQtral-1** satellite (developed by Thales Alenia Space) will be launched in 2024
- **QEYSSat** will be Canada's first QKD satellite planned to be launched in 2024-2025
- **Hispasat** is defining a GEO QKD mission that will fly as hosted payload in 2025

European Quantum Communication Infrastructure

EuroQCI aims to build a network of quantum secure shield that will include:

- ❑ Quantum Key Distribution (QKD) Satellites
- ❑ Optical Ground Stations (OGS)
- ❑ Ground Infrastructure – A Trusted Network



Greece became part of EuroQCI at the end of 2019

Greece's key partners

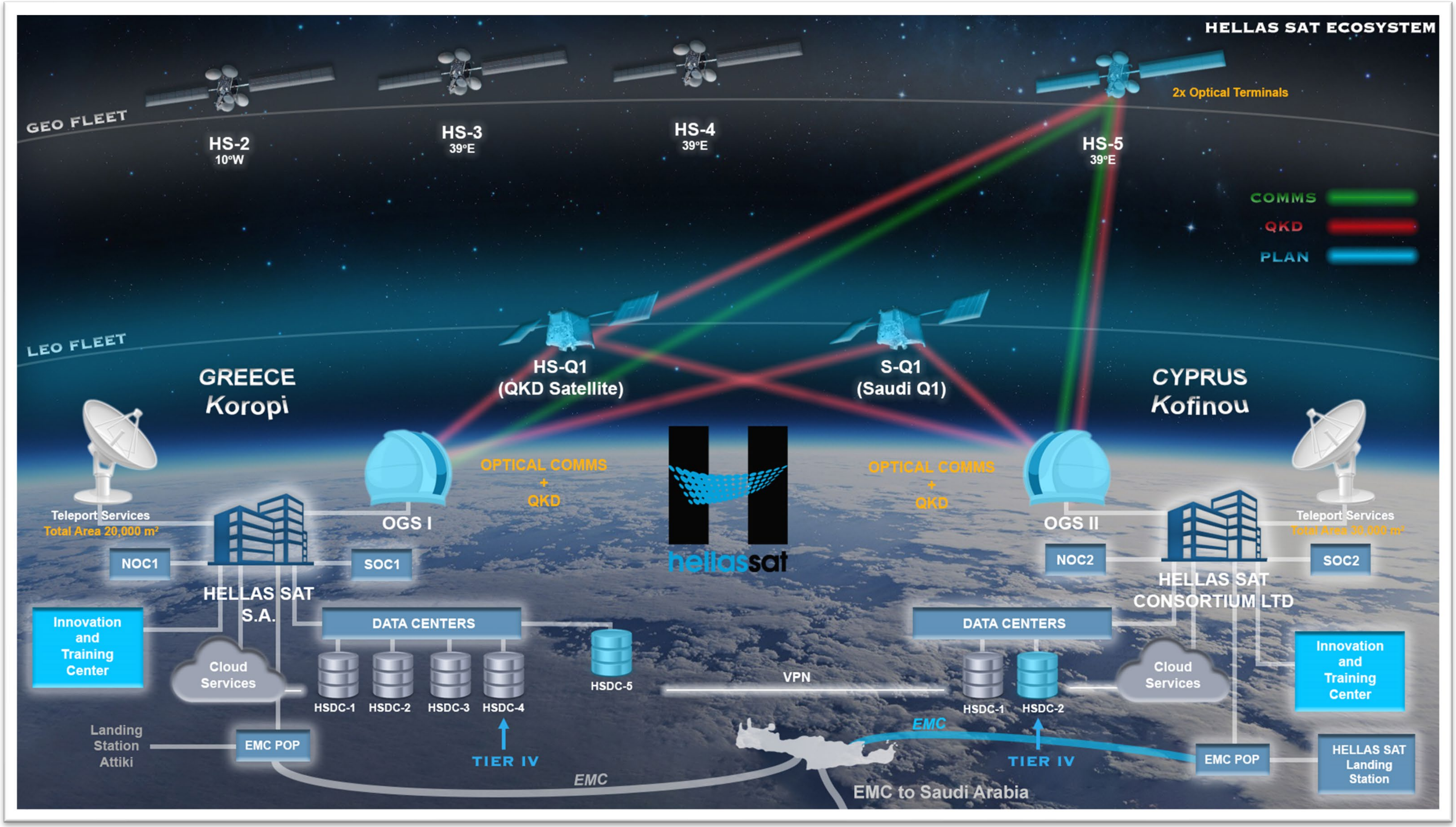
- Ministry of Digital Governance (MinDig)
- Ministry of Defence (MoD)
- National and Kapodistrian University of Athens (NKUA)
- Institute for Astronomy, Astrophysics, Space Applications and Remote Sensing (IAASARS)
- Foundation for Research and Technology (FORTH)
- Aristotle University of Thessaloniki (AUTH)
- National Centre for Scientific Research Dimokritos (NCSRD)
- National Observatory of Athens (NOA)

Hellas Sat – National Observatory of Athens MoU

Athens, 17 April 2022 - **Hellas Sat and the National Observatory of Athens have signed a Memorandum of Understanding and Cooperation to exchange knowledge and information in the area of Space Situational Awareness**

- Bridging the knowledge between the two parties
- Exchange information on key area of Space Situational Awareness scenarios
- Perspective for future tighter cooperation to solidify Space Situational Awareness National autonomy
- Open doors to Nationally independent satellite tracking and survey operations

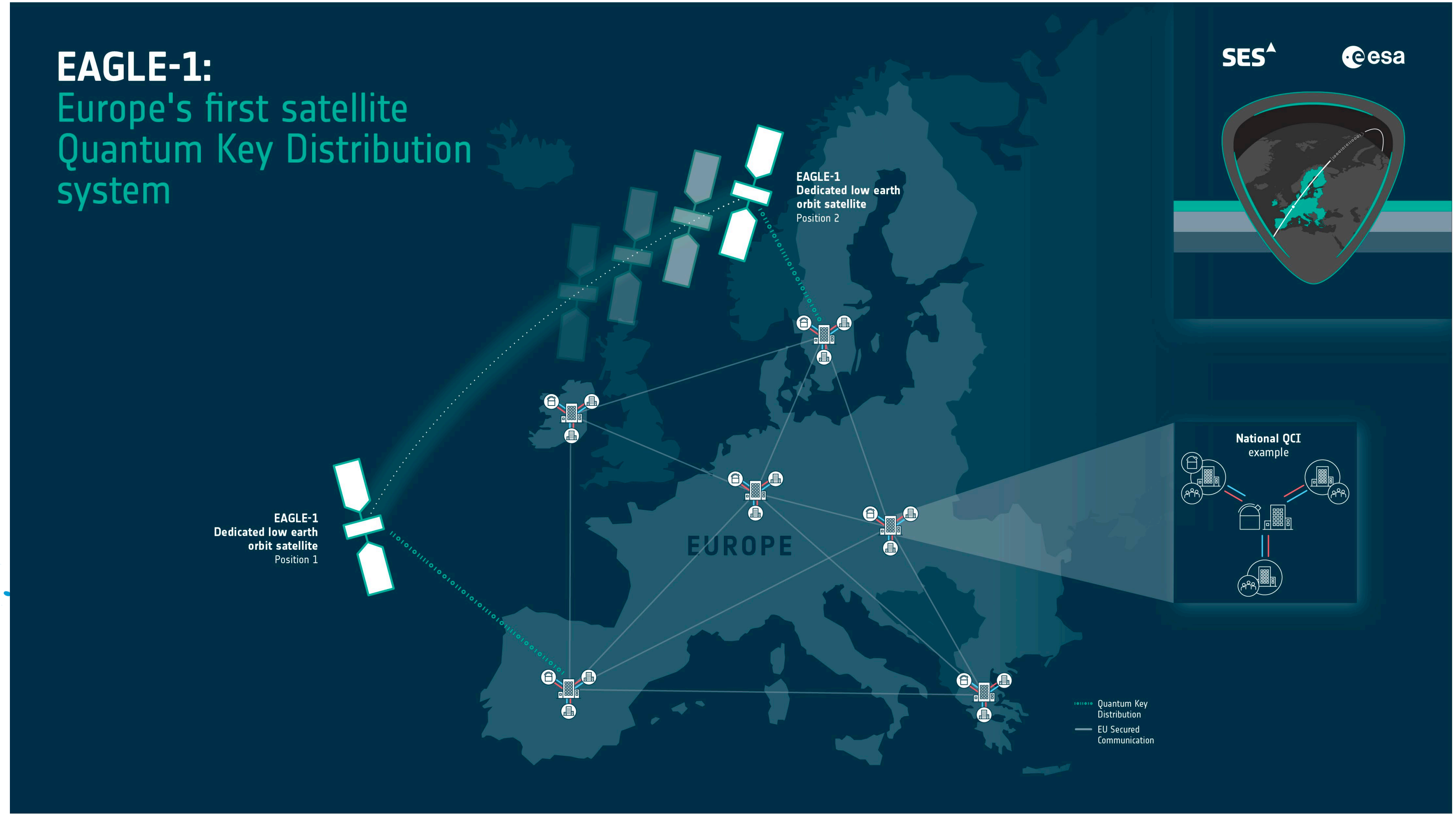
Hellas Sat – Quantum Expansion



Thank You!

APPENDIX

European Quantum Communication Infrastructure



Quantum Computing vs Classical Computing