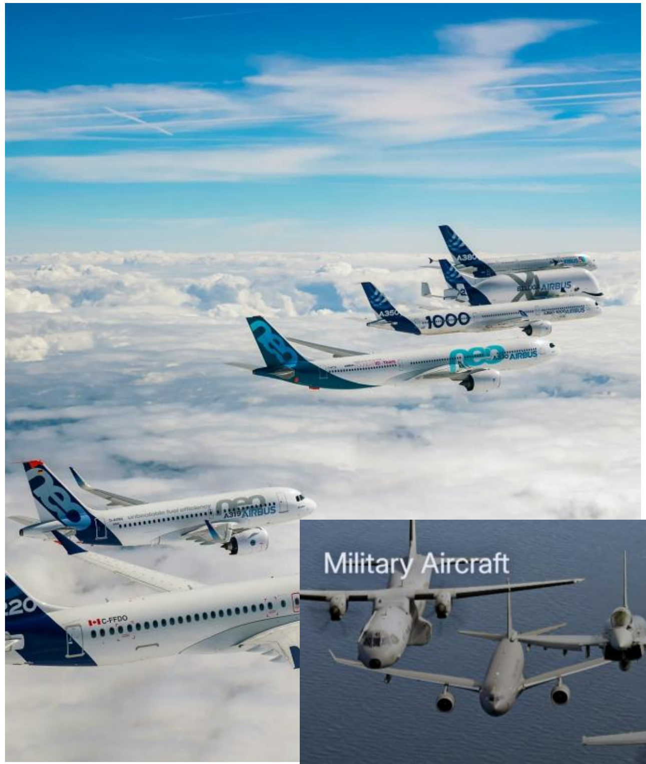
Quantum Security Unleashed:
A New era for Secure Communication and Systems

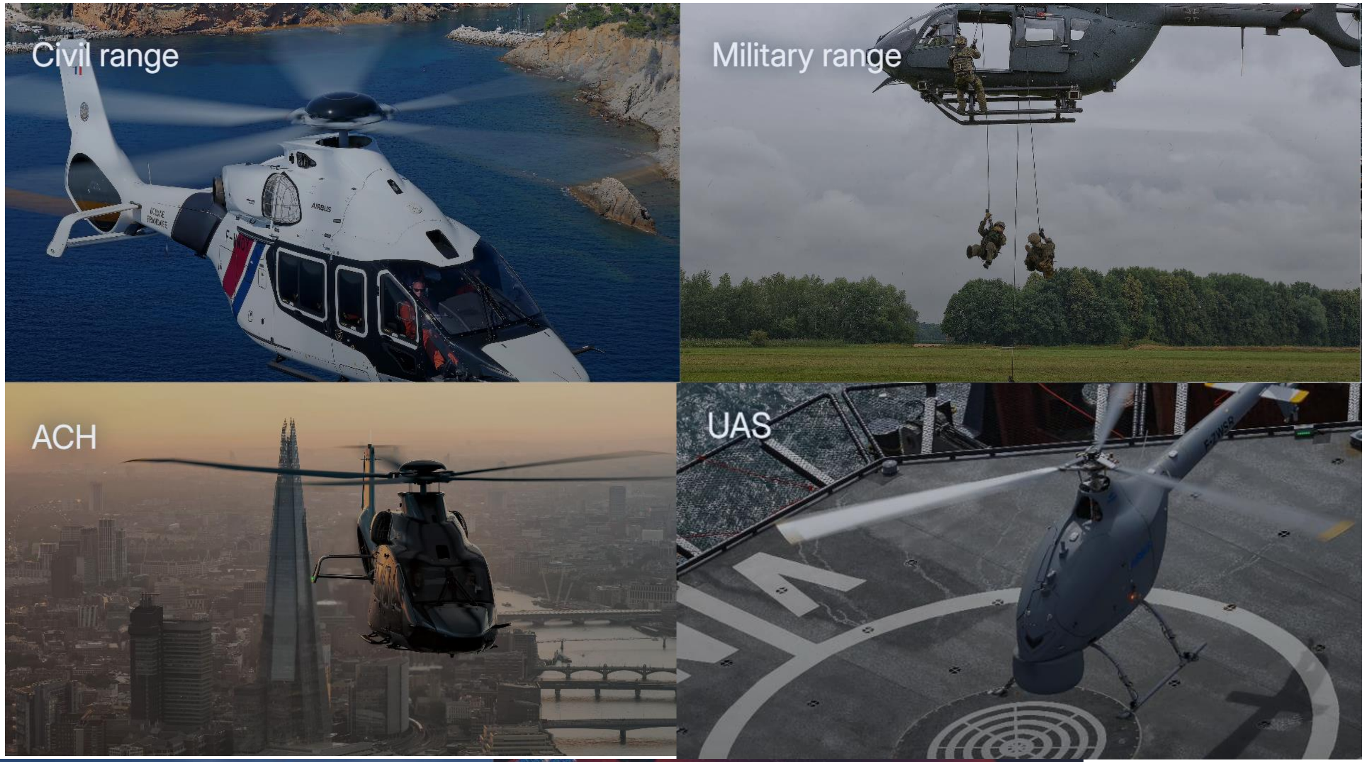
DEFENCE AND SPACE

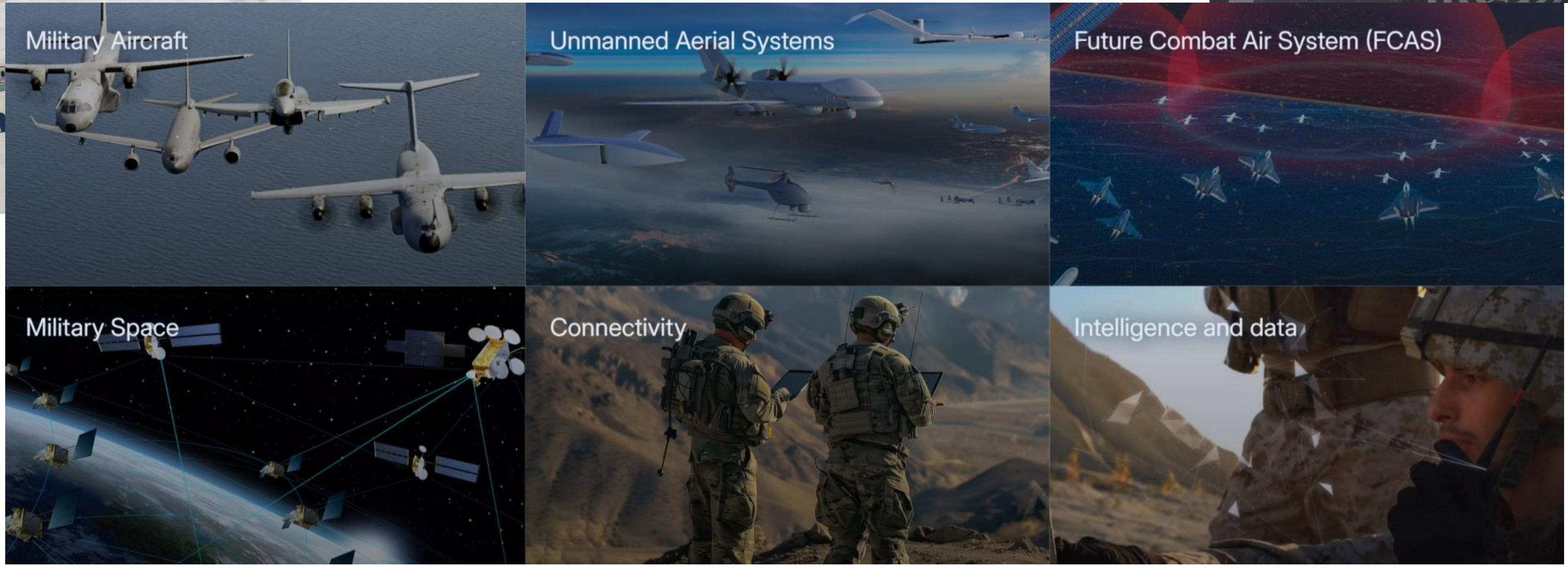
Johanna Sepúlveda, Ph.D.
Senior Expert Quantum Secured Communications
Chief Engineer Quantum Technologies

AIRBUS

Airbus

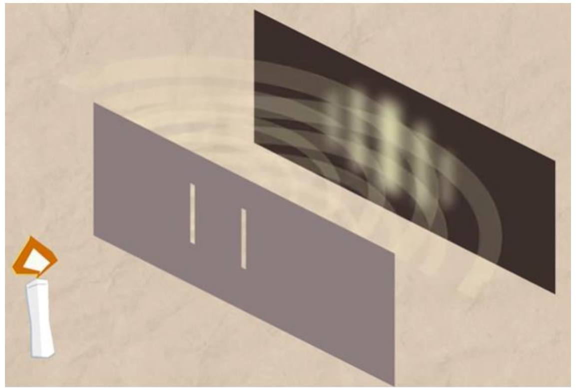



Civil range
Military range
ACH
UAS

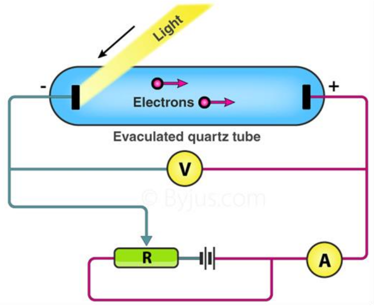

Military Aircraft
Unmanned Aerial Systems
Future Combat Air System (FCAS)
Military Space
Connectivity
Intelligence and data

Quantum Technologies Principles and General View

Quantum Technologies: **First Revolution**

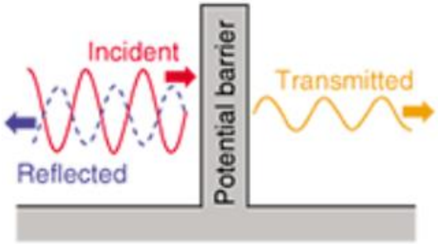


Experiment of Young
(Wave nature of light)



Photoelectric Effect
(Particle nature of light)

Wave-Particle Duality (1905)



$$\boxed{\Delta x \cdot \Delta p \geq \frac{h}{4\pi}}$$

Position Uncertainty

Momentum Uncertainty
(p=m.v)

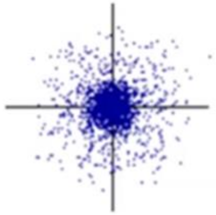
Planck Constant

The position and the velocity of an object cannot both be **measured** exactly, at the same time

Uncertainty Principle of Heisenberg (1927)

$$\boxed{-\frac{h^2}{8\pi^2 m}\left(\frac{\partial^2\psi}{\partial x^2}+\frac{\partial^2\psi}{\partial y^2}+\frac{\partial^2\psi}{\partial z^2}\right)+V\psi=E\psi}$$

$(\psi)^2$: Electronic probability density

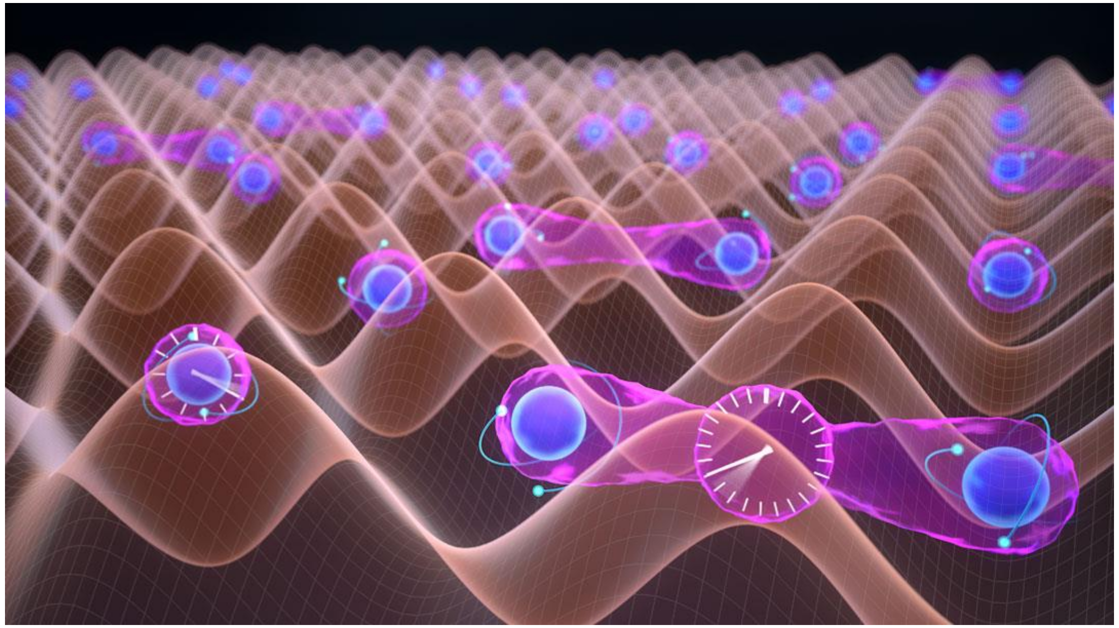


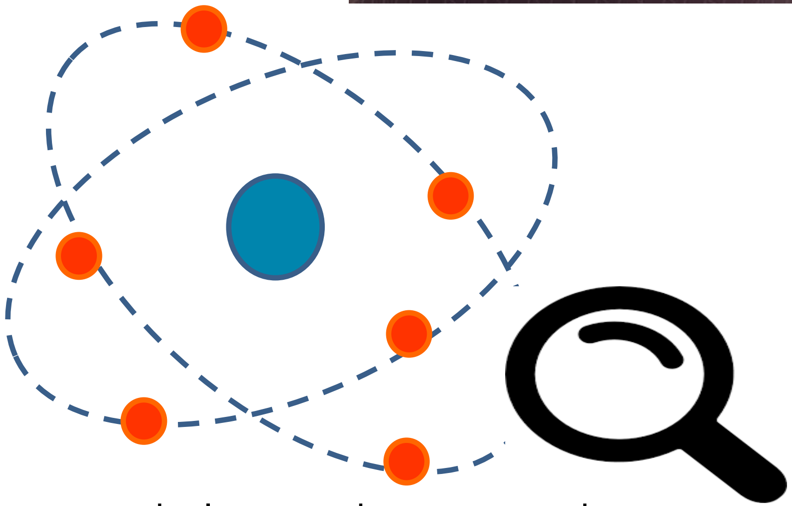
Orbitals: Described by **quantum numbers** (n l m_l m_s)

Function that describes the state of a quantum-mechanical system

Schrödinger Equation (1925)

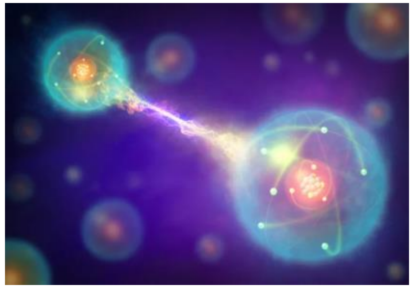
Quantum Phenomena





Collapses to a single state when measured

Superposition



Entanglement

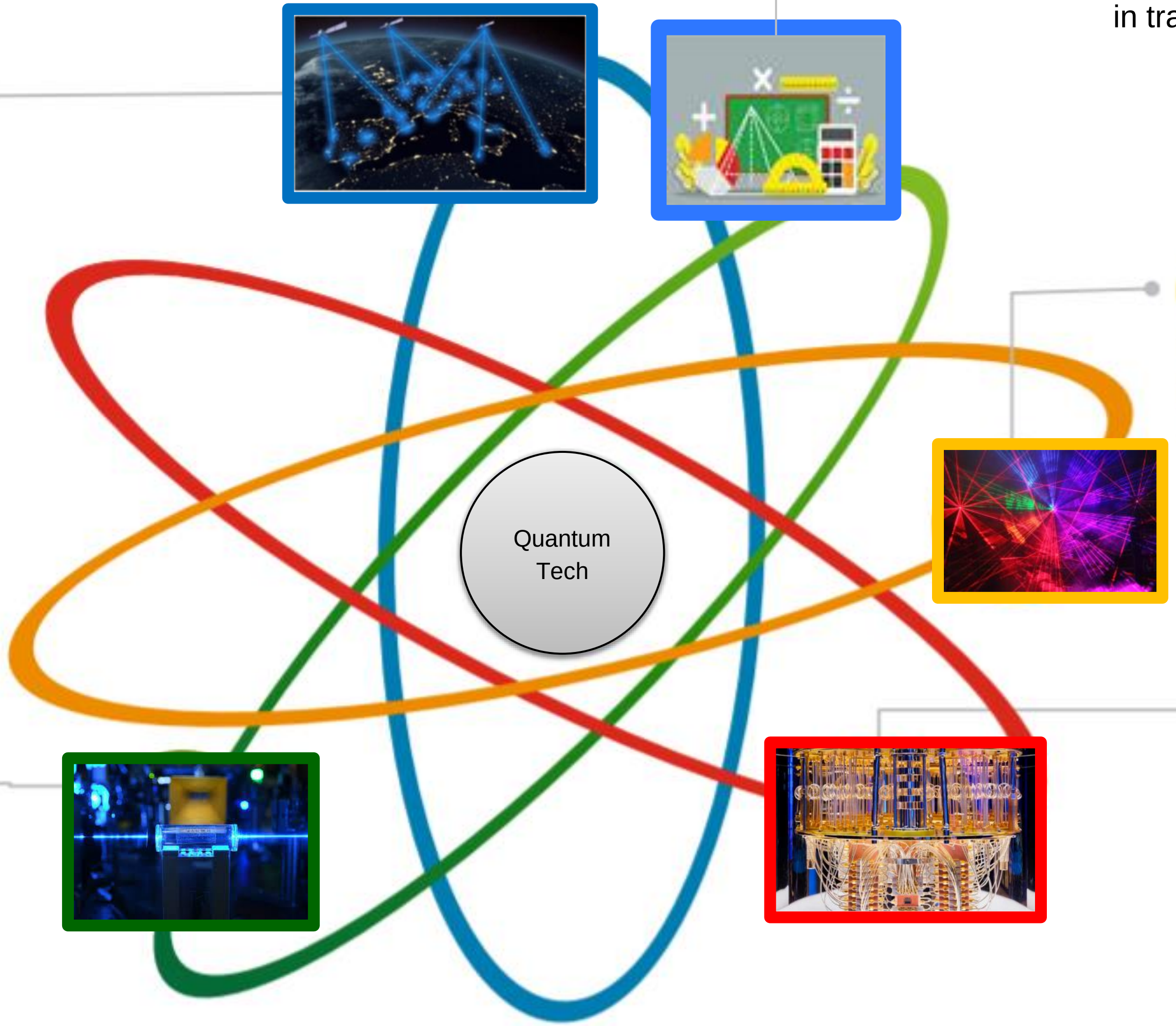
Quantum Technology: **Second Revolution**

Quantum Communications

Quantum communications protects data that flows through optical fibre or wireless communications, by using quantum encryption.

Post-Quantum Cryptography

Cryptographic algorithms that can be deployed in traditional devices and



Quantum Enabling Technologies

Technologies that comprise a quantum system or the value-chain for the quantum technology industry, such as lasers, optics, semiconductors...

Quantum Sensing

Precise measurement of the environment, using very accurate quantum based sensors.

Quantum Computing

Quantum computing will enable solving highly complex computation problems. Research focus on both hardware and software. Building universal quantum computers and specific simulators.

McKinsey Report 2022

General Market View: Quantum Technologies (QT) World Map

The QT market is still dominated by North America

North America leads the QT market, with nearly 40% of players and over 60%[1] of all start-up funding

10 out of the 12 biggest hardware players are based in North America

China leads in commercial implementation of QComms. Japan is the front-runner in QT industry adoption

Funding is rising rapidly

Announced raised funding for 2021 (~$2.1 bn) is already almost triple the total funding of nearly $800 m raised in 2020

Announced major deals for 2021 extend to software and QComms players

China has committed $15 bn over 5 years for QT; the European Union announced $7.2 bn

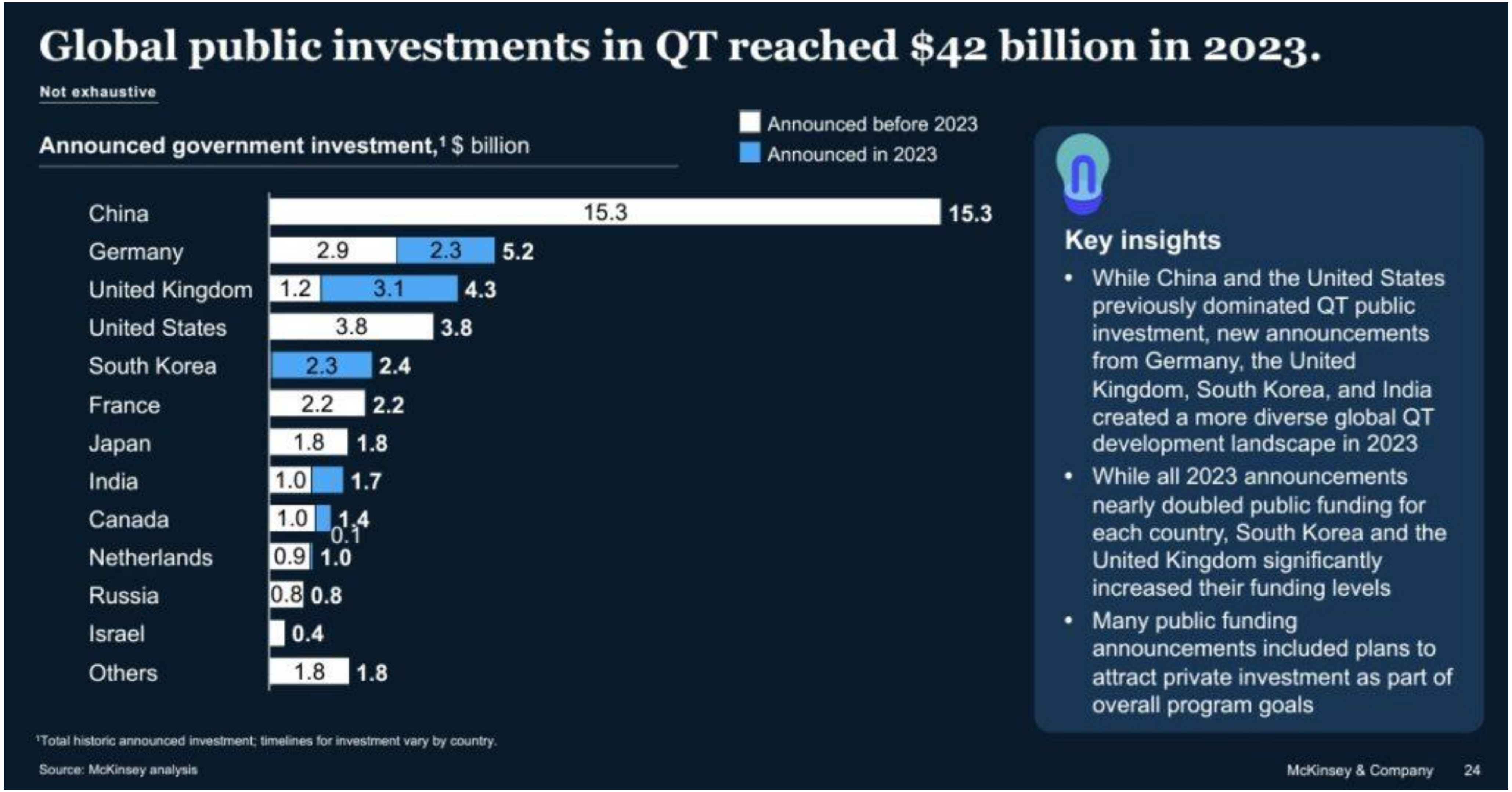
Global market participation is increasing

The United Kingdom is catching up to North America due to recent major deals

China leads in patents and is expected to catch up rapidly on QC

AIRBUS

General Market View: Quantum Technologies (QT) Funding



McKinsey Report 2023

General Market View: Quantum Pillars

+XX% Compared to previous year

Quantum computing
- 261 start-ups
- $6.7 billion investment

Quantum communication
- 96 start-ups
- $1.2 billion investment

Quantum sensing
- 48 start-ups
- $0.7 billion investment

Companies pursuing two or more quantum technologies simultaneously: 38

Technological breakthroughs in 2023

Quantum computing
Quantum error-correction proposals and demonstrations by large players accelerate timelines toward large-scale, fault-tolerant quantum computing

Quantum communication
Improved performance for quantum key distribution, and demonstration of longer transmission distances and increased data rates for quantum networks

Quantum sensing
Development of new techniques to improve the sensitivity of quantum sensing devices

Scientific progress

4,763 +1% YOY
QT-related patents granted in 2022[1]

42,155 –4.5% YOY
QT-related publications in 2023

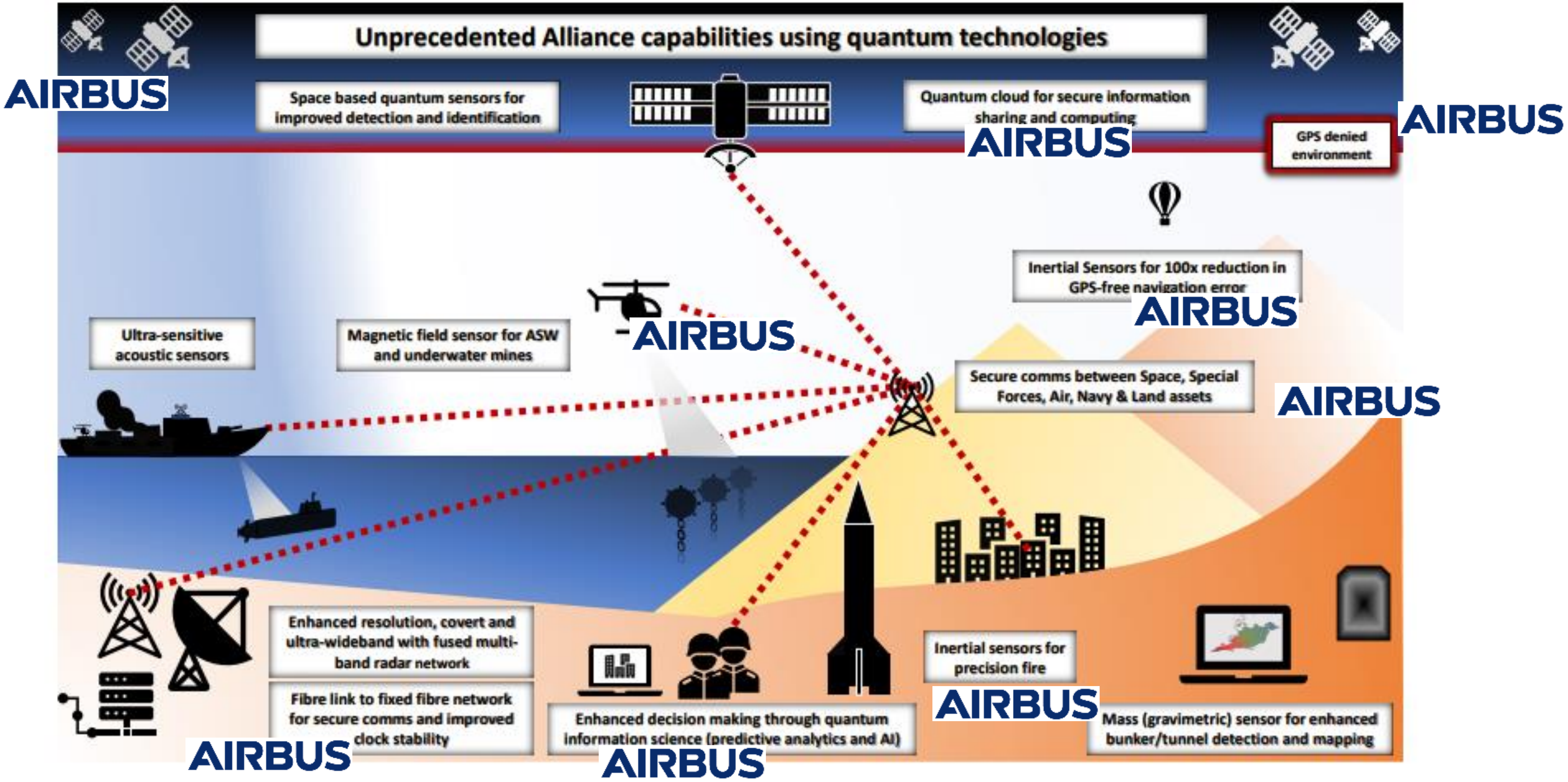
Quantum-capable talent

55 +10% YOY
QT master's degree programs

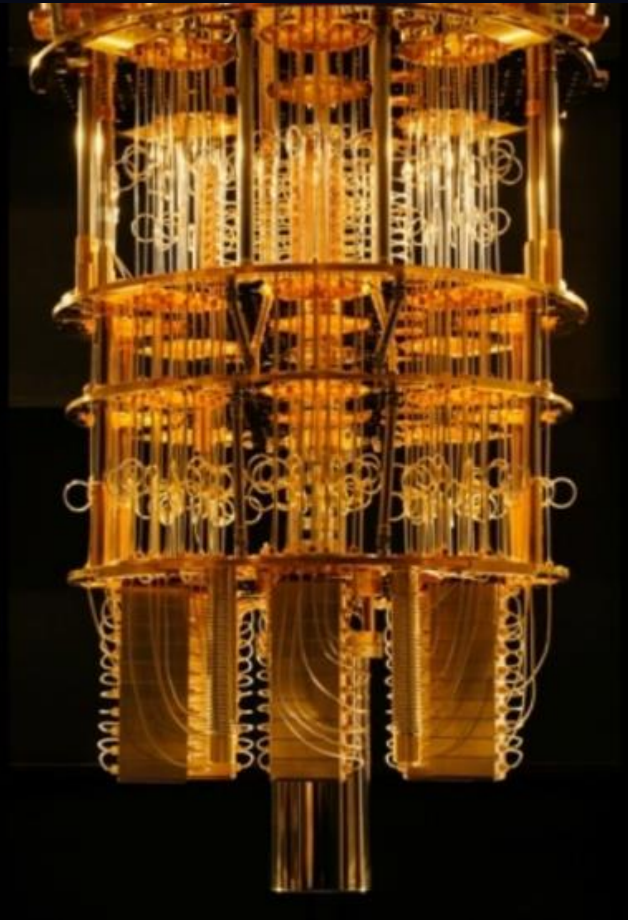
195 +8.3% YOY
universities with QT research groups

AIRBUS

NATO Quantum Capabilities and Airbus Footprint



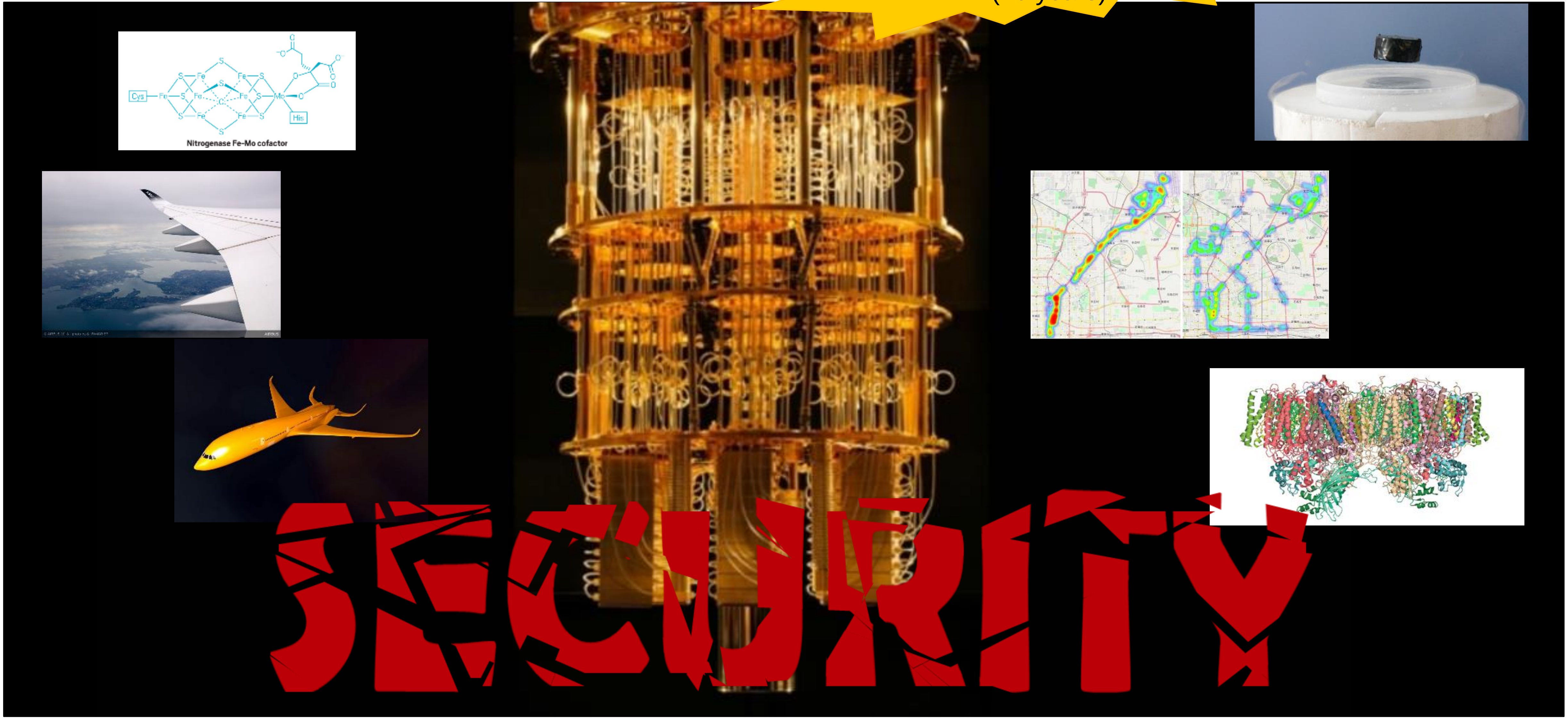
Quantum Technologies Principles and General View



Quantum Computers

Quantum Computer

When?
At any moment!
(10 years)



Quantum Threat

QU

SKC/PKC in CLASSIC

Better classic algorithm

~ 10^{34} Steps

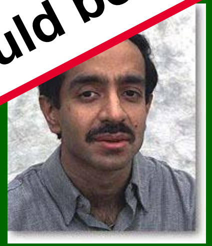
In a ***classic computer*** (*THz*)

(1 trillion of ops / sec)

~ 17 Trillions of years

AES

Key size should be doubled



Grover's algorithm

Halves the security of AES

AES-128 → AES-256

Shor's algorithm

~ 10^{7} Steps

Solves PKC

In a ***quantum computer*** (*MHz*)

(1 million of ops / sec)

~ 10 Seconds

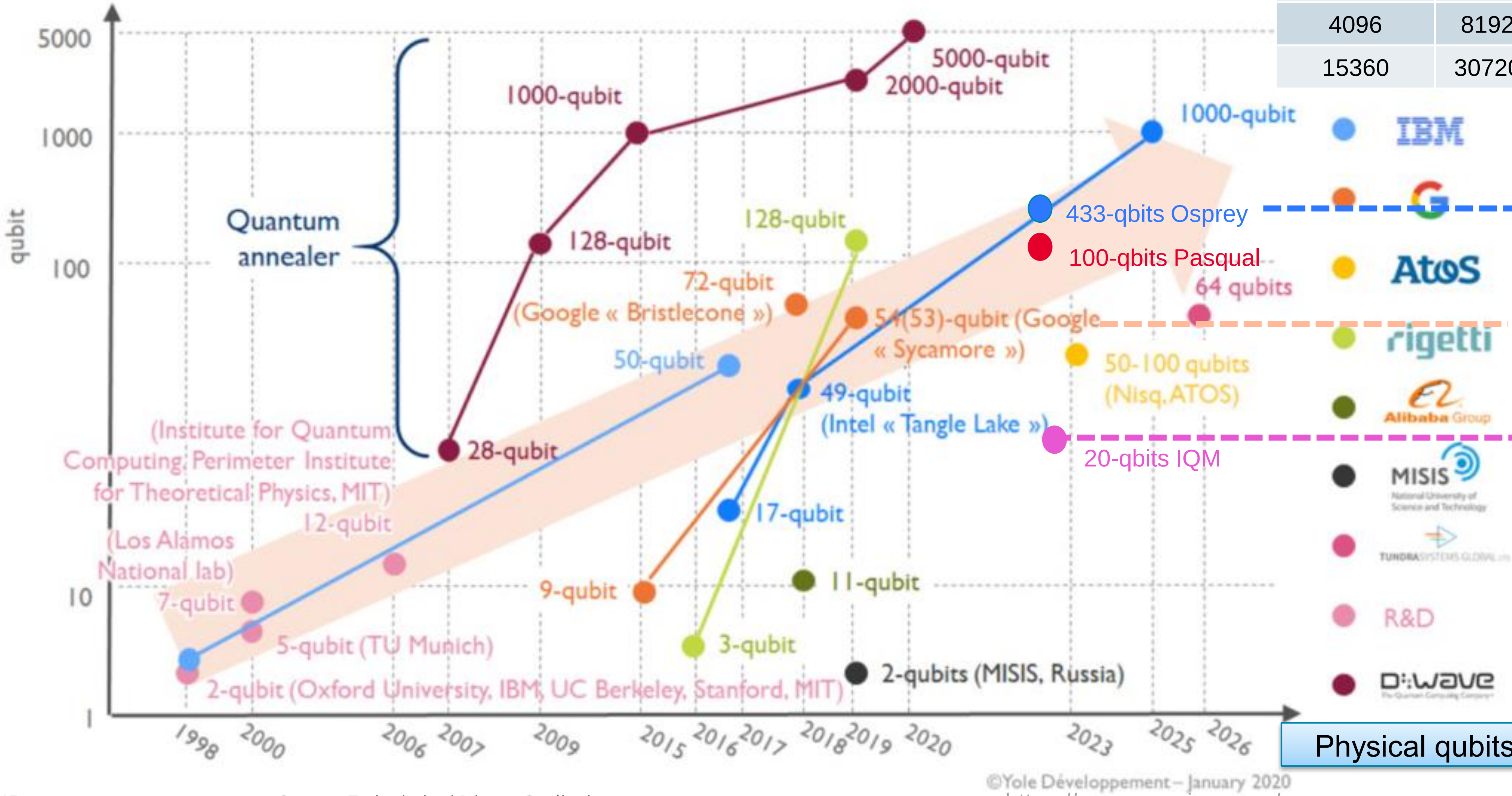
PKC

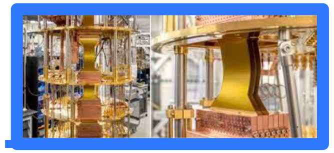
New algorithms/methods

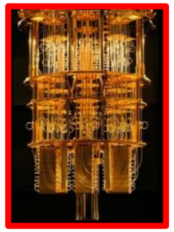
AIRBUS

Quantum Computer Roadmap

RSA		ECC	
Key Length	qubits	Key Length	qubits
1024	2048	163	1000
2048	4096	224	1300
3072	6144	256	1500
4096	8192	383	2300
15360	30720	512	3000





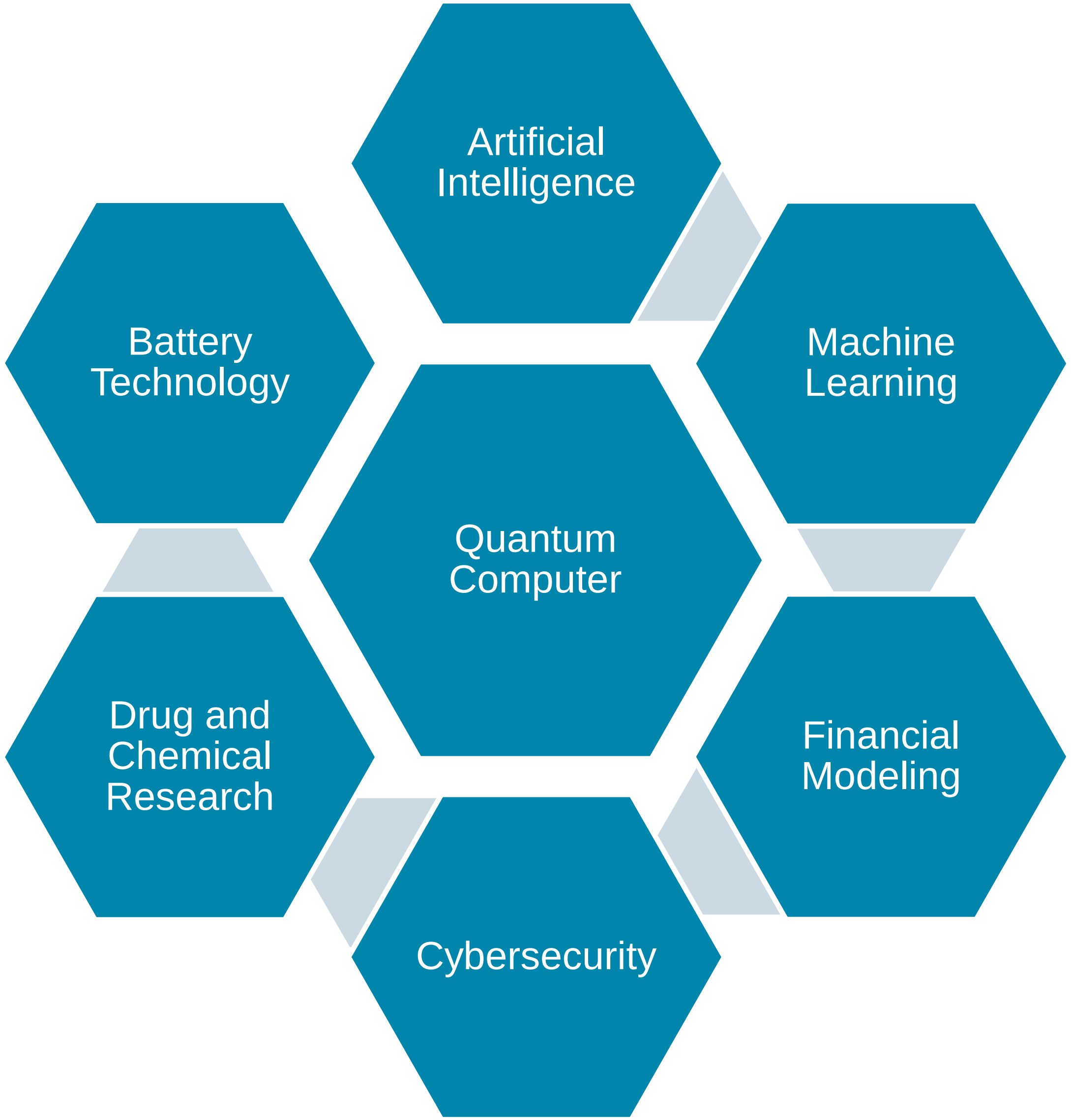


Physical qubits ≠ Operational qubits

https://www.grss-ieee.org/

AIRBUS

Applications



- ✓ Internet-of-Things
- ✓ Language Processing
- ✓ Logistics and optimization

Network monitoring/ Smart scheduling

Cryptanalysis

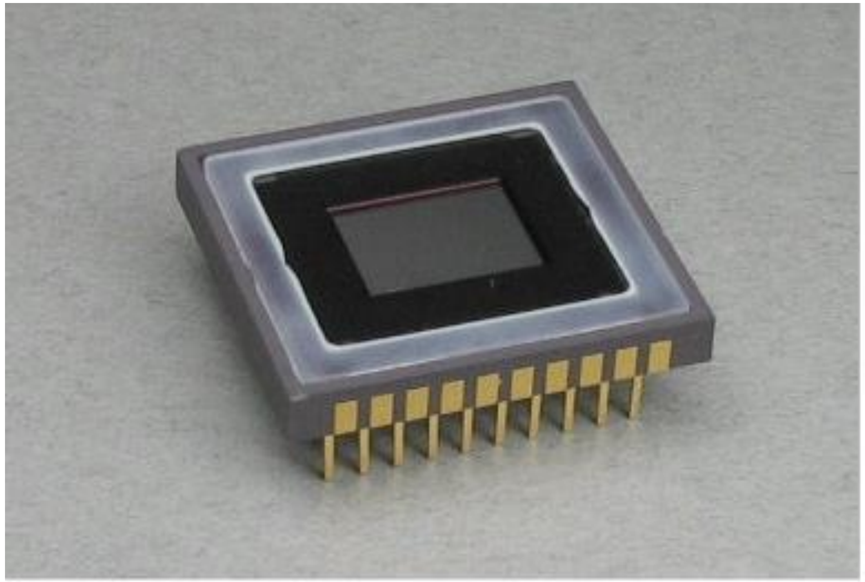
AI/ML based implementation attacks

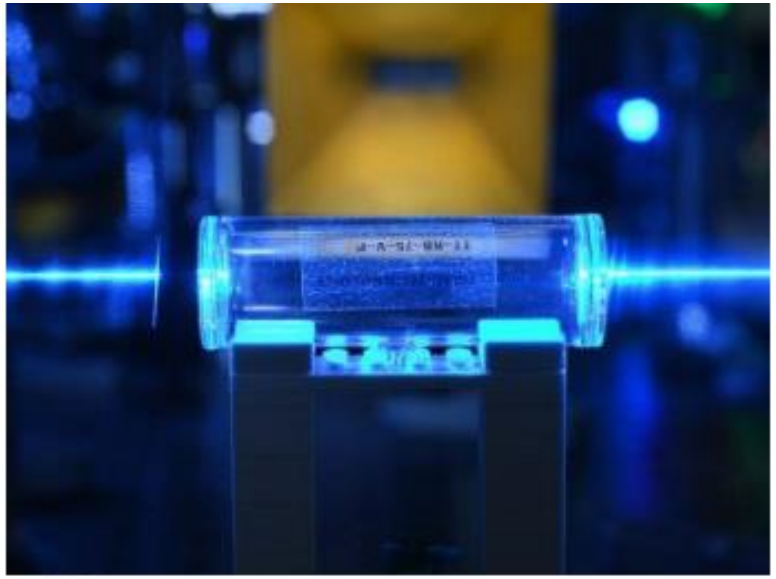
Pattern Recognition

Threat Detection

Quantum Sensing

Classical Sensors Vs Quantum Sensors



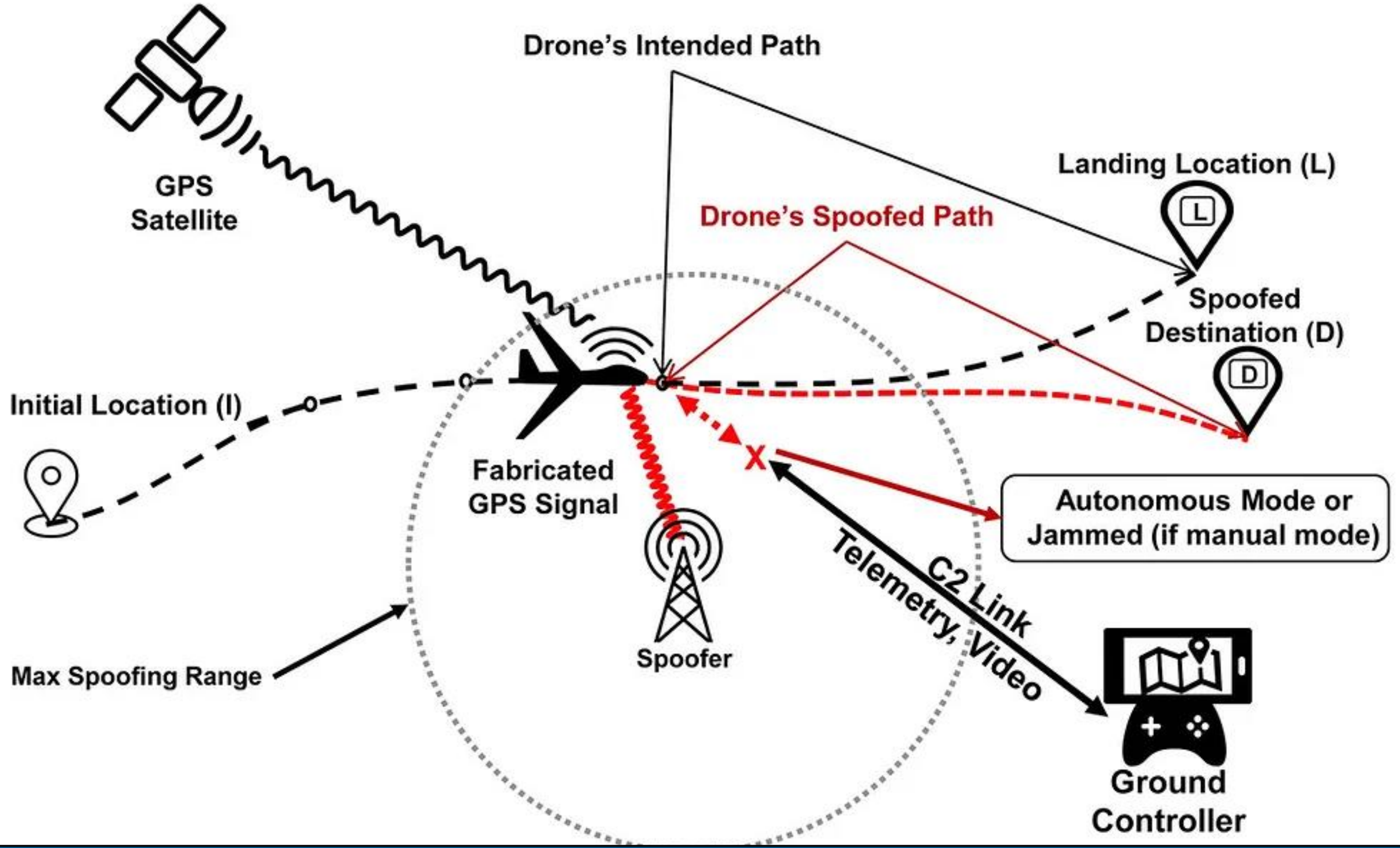


More sensitive	High Precision	High Stability	Low Maintainance

Measures the same physical quantities as classical sensors but through the exploitation of quantum phenomena

Current challenges: Jamming and Spoofing (OODA)

GNSS: Global Navigation Satellite System



GNSS is not always available; such as underwater, urban, or hostile environments

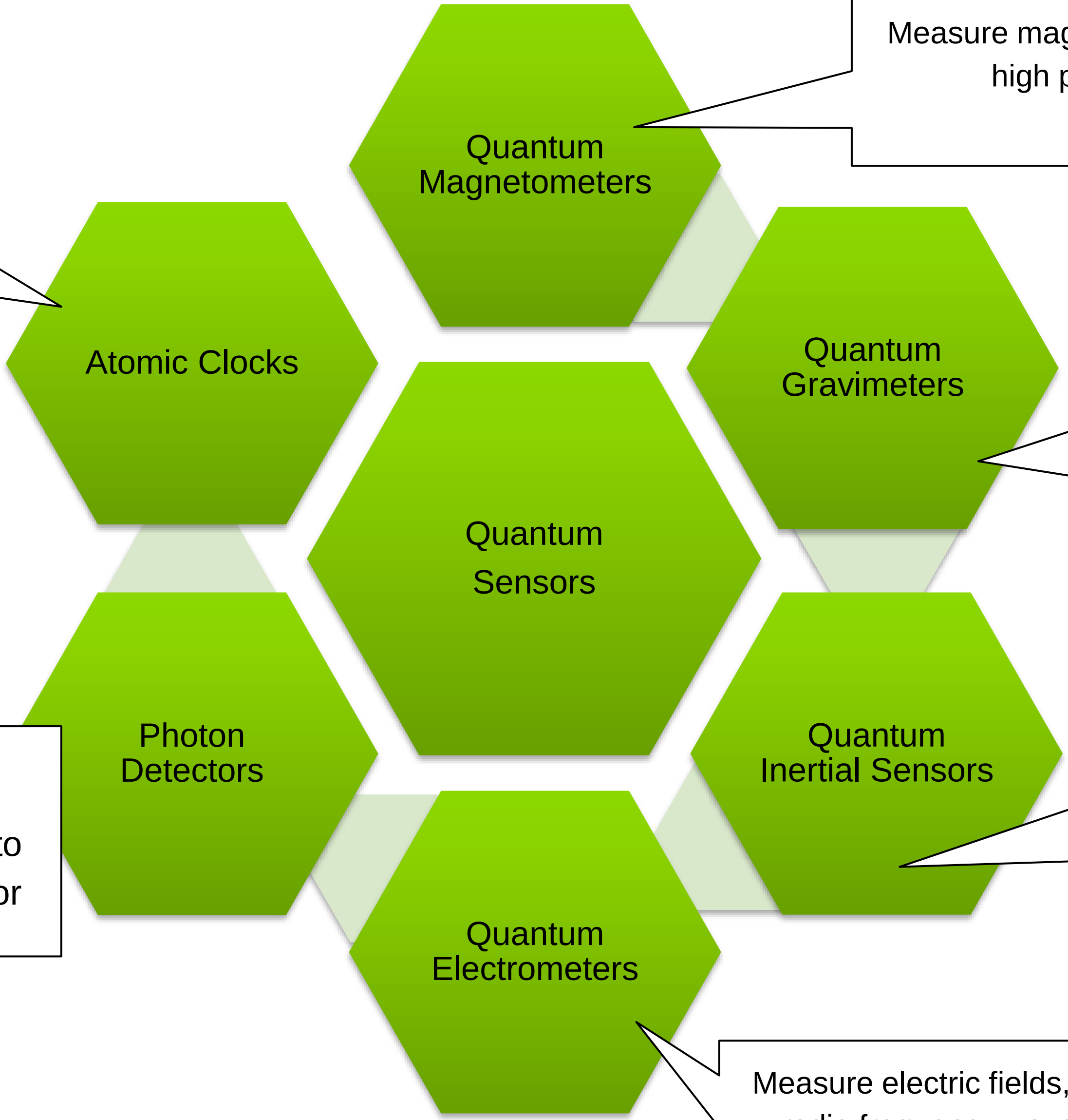
GNSS spoofing attack is less expensive (from 50 – 500 USD to 100 USD)

Quantum Sensors

Measure magnetic fields with high precision

The most accurate timekeeping devices ever created

Measure the strength of local gravitational acceleration using quantum interference.



Enable three-dimensional imaging based on the time it takes a photon to travel between an object and detector

Quantum accelerometers and quantum gyroscopes, which measure changes in linear acceleration and rotation using the principles of quantum interference

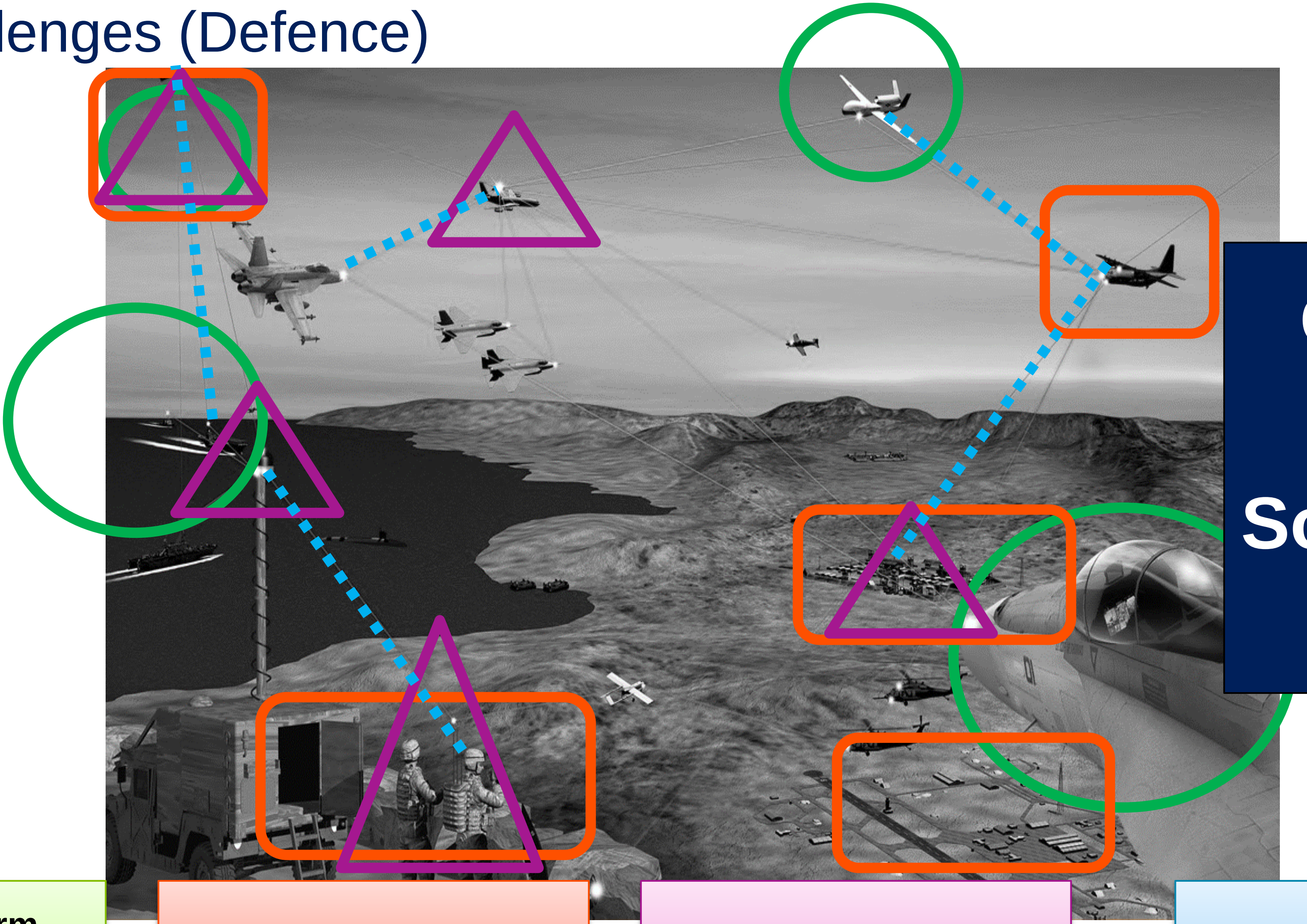
Measure electric fields, such as the radio frequency waves used by effectively all modern communication devices.

Quantum Sensors Applications: Gravity Cartography, Navigation, Advanced SCA

AIRBUS

Quantum-Secure Communication

Security Challenges (Defence)



Quantum-Secure Solutions are required

Require long term security

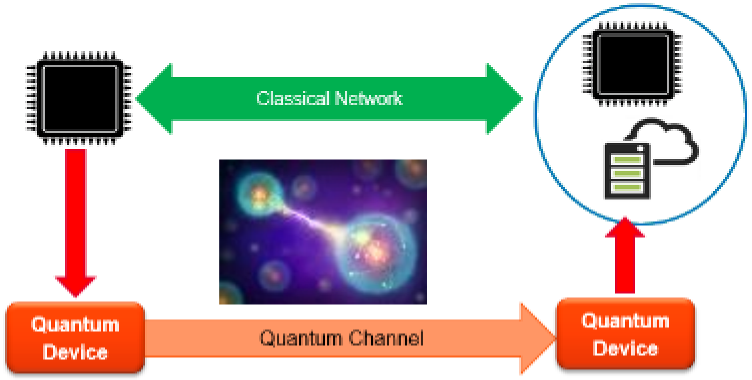
Criticality

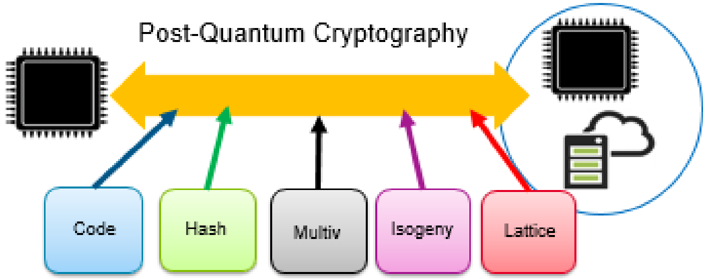
Heterogeneity

Different Communication capabilities and needs

Quantum Key Distribution (QKD)

Post-Quantum Cryptography (PQC)





Goal:

Use a quantum channel to transfer **a secret random key.**

It is **impossible** that an attacker read (measure) without getting noticed

Goal:

Protect the communication through **hard mathematical problems** resistant to traditional attacks and quantum attacks

Transition: Layered approach (different layers of protection)

Post-Quantum Cryptography

Code | Hash | Multivariate | Isogeny | Lattice

Post-Quantum Cryptography (PQC) Types

Code-based

(e.g. McEliece)

Pros:

- Well studied error correcting codes
- Multipurpose
- Fast

Cons:

- Very large key sizes

Hash-based

(e.g. SPHINCS)

Pros:

- Security relies on hash functions
- Very efficient

Cons:

- No encryption schemes
- Track of signed messages

Multivariate

(e.g. GeMSS)

Pros:

- Multipurpose
- Very efficient for signature schemes

Cons:

- Most public key schemes are broken

Isogeny

(e.g. SIKE)

Pros:

- Elliptic-based
- Smallest key sizes

Cons:

- Low efficiency
- Difficult to construct

Lattice-based

(e.g. NTRU, LWE, RLWE)

Pros:

- Efficient
- Public key, digital signatures, FHE, IBE

Cons:

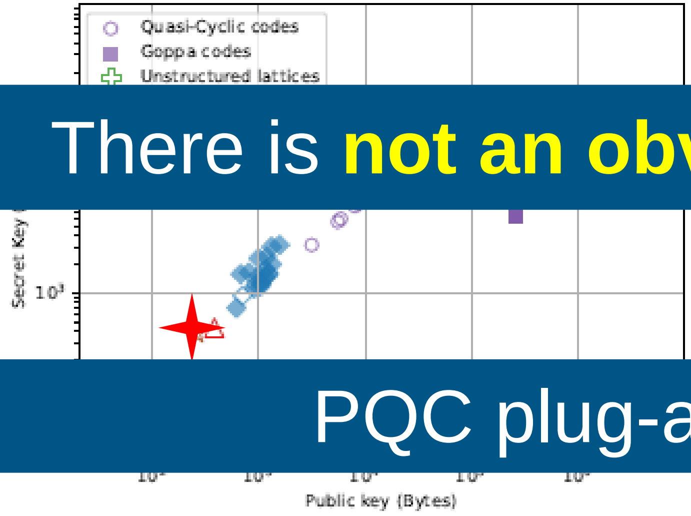
- Key sizes when compared to classical crypto

AIRBUS

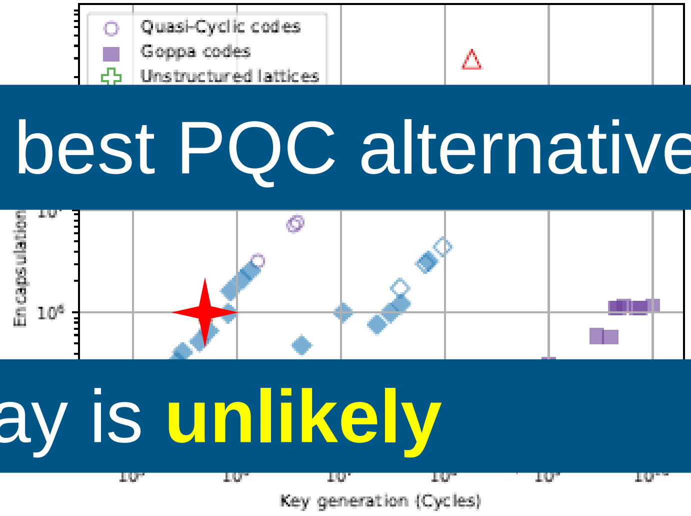
PQC Benchmarking “Example”

NIST

Key Sizes



Performance



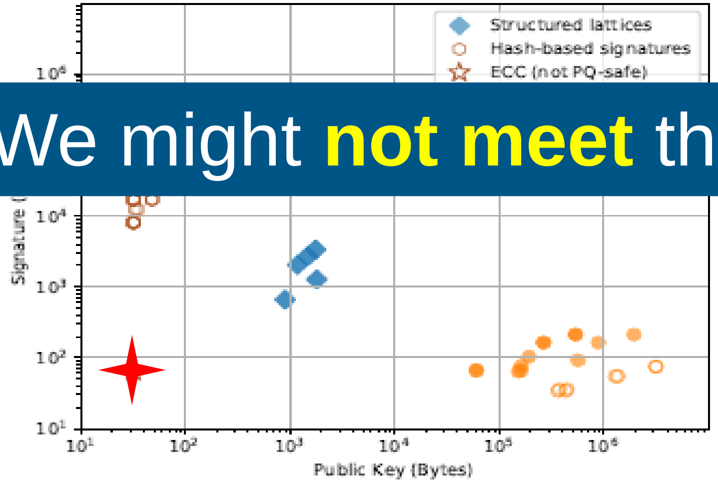
There is not an obvious best PQC alternative

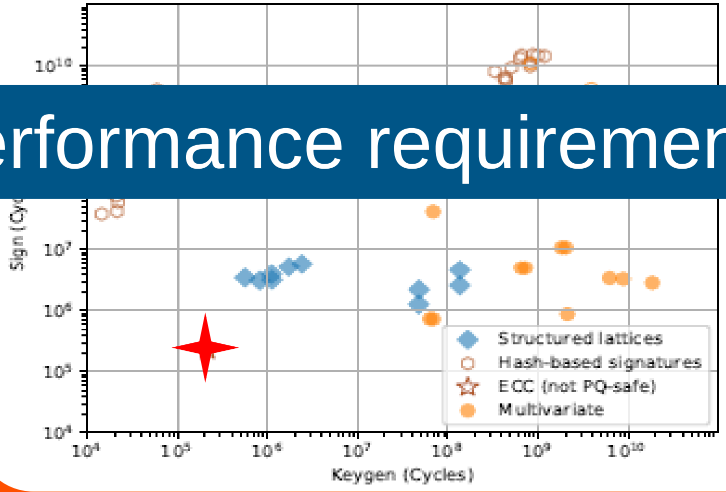
PQC plug-and-play is unlikely

KEM

Signature

Use Case





We might not meet the performance requirements

AIRBUS

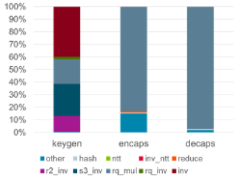
Airbus PQC Innovation and Footprint

National Institute of Standards and Technology (NIST) PQC standardization Roadmap

2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | Future

Apr.16:
NISTIR 8105
report

Dec.16:
Formal call for
submissions



…7:
…round
candidates
announced

Nov.17:
Deadline fo
submission

Airbus:
Ultra-constrained
PQC solution

Airbus: First
PQC-codesign HW/SW
(Crypto-agility)

Apr.18:
First NIST
…C Workshop

Airbus: First
PQC-enhanced
Wireless sensor
network

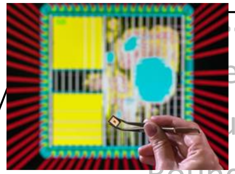
Second-round
candidates
announced

Aug.19:
Second NIST
PQC Workshop

Jul.20:
Third-rour
candidate
announce

Airbus:
Record on PQC
Implementation
(performance, power,
memory footprint)

Airbus:
Design 1st Chip with EU
processor with PQC



Jun.21:
Third NIST PQC
Workshop

…22:
…ed PQC
…unced;
Round four
begins

Jul.22:
Formal call
new signature

Airbus:
Record implementation of
advanced PQC
crypto-primitives

…23:
Fi…
…C draft
…ished

Airbus:
Demonstration
PQC on the
field
Secure Drone
Connectivity

Jun.23:
Deadline for
submissions
…v signatures

…024:
Publ…on
S…

Airbus:
Development of
advanced
PQC-enhanced
systems
Space, dynamic
networks, PQC-
secured Blockchain

AIRBUS

Quantum Cryptography

QKD Network: Terrestrial and Space segments

To deliver keys between different communication parties (identical, private)

- **Terrestrial**: Optical fibre or free-space ground-to-ground optical links

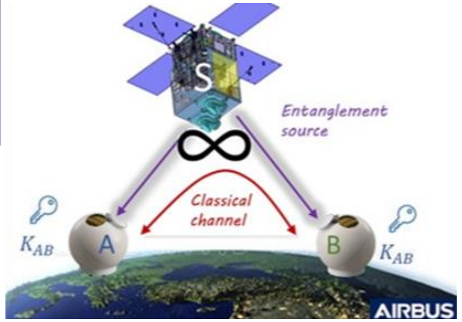
  Higher throughput, limited coverage (maximum distance between consecutive nodes is 100km)
- **Space**: free-space satellite links

  Low throughput but high coverage (LEO)

Two QKD nodes

FSO for terrestrial segment

Protocol 1: Prepare and Measure

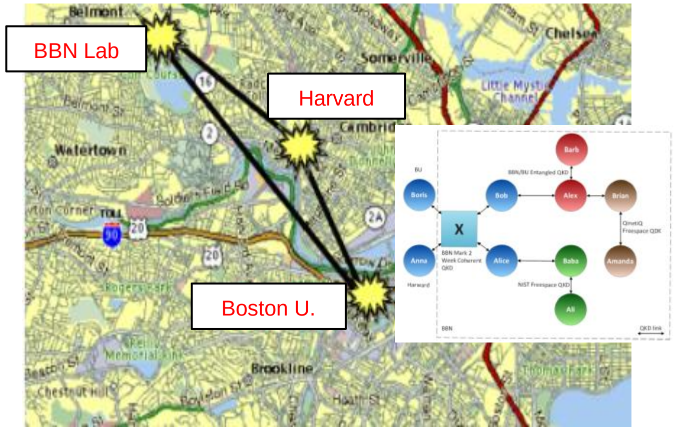


Protocol 2: Entanglement

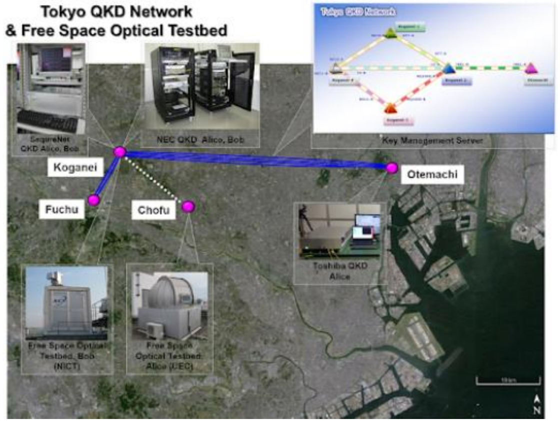
AIRBUS

Worldwide Demonstrations (terrestrial)

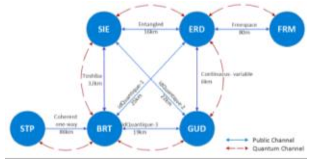
DARPA (2002)



TOKYO (2009)



CAMBRIDGE (2019)

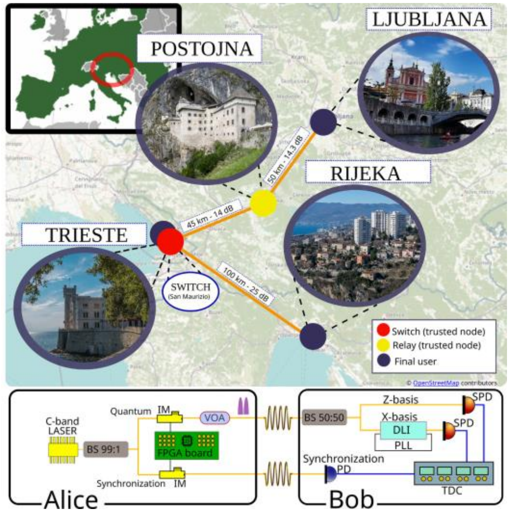


SECOQC (2008)

SOUTH KOREA (2015, 2017, 2020)

B

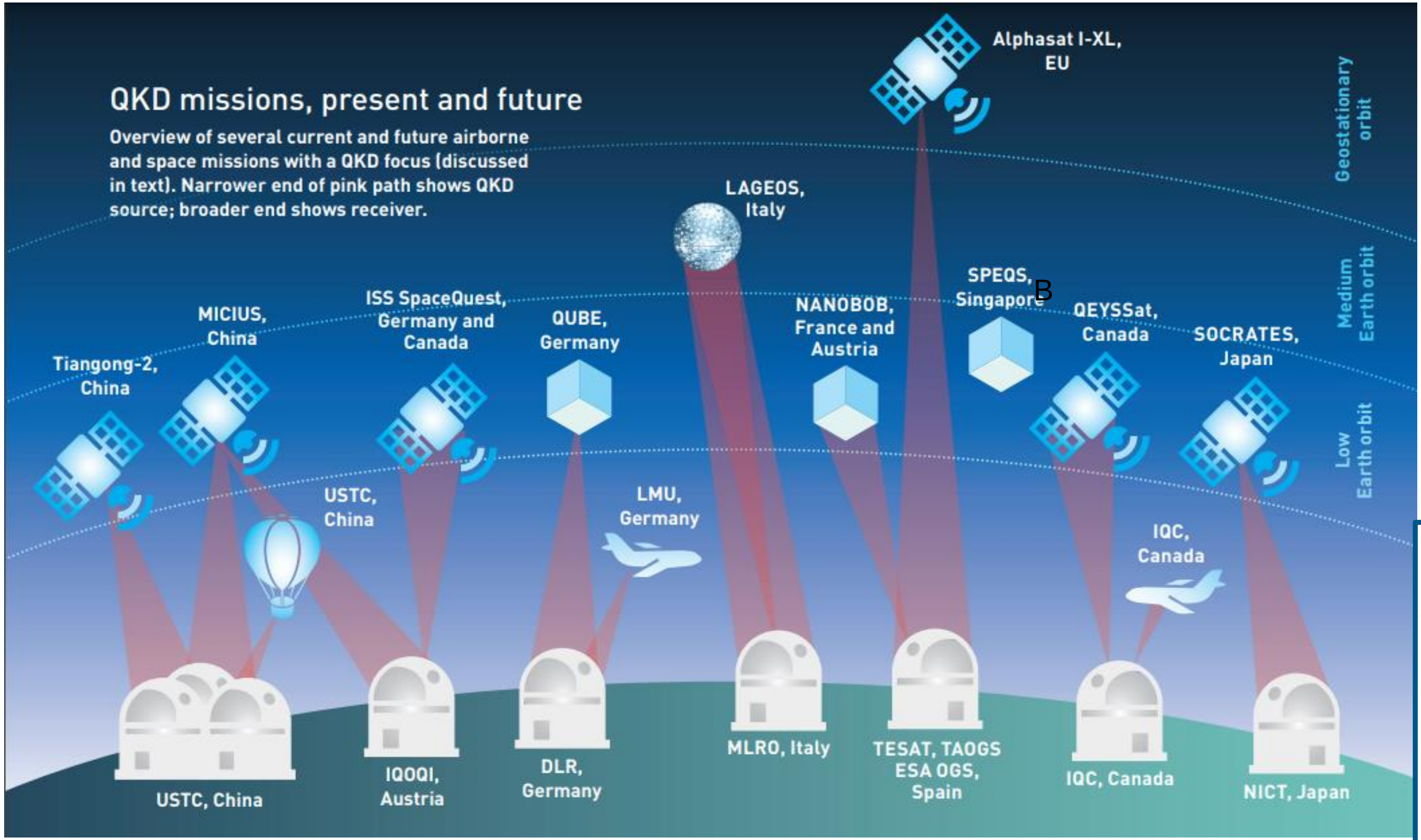
ITALY-IQB INRIM CNR (2018)



ITALY-SLOVENIA-CROATIA (2021)

AIRBUS

Worldwide Demonstrations (Space)



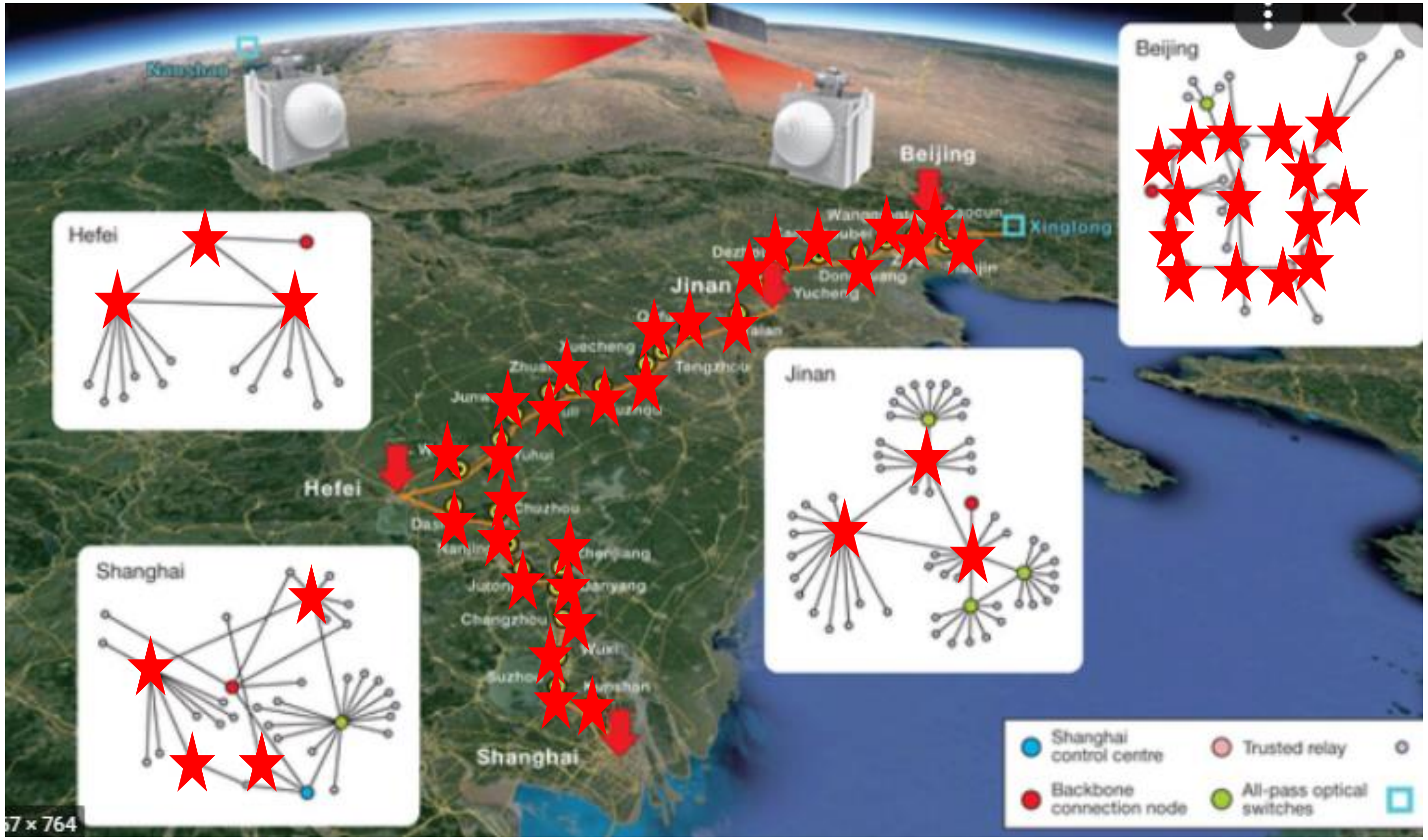
I. Khan et al. Satellite-based QKD. Optics and Photonics News. 2018

Airbus Drone

Q-DOS (UK)

AIRBUS

Chinese QKD Network: Terrestrial And Space QKD

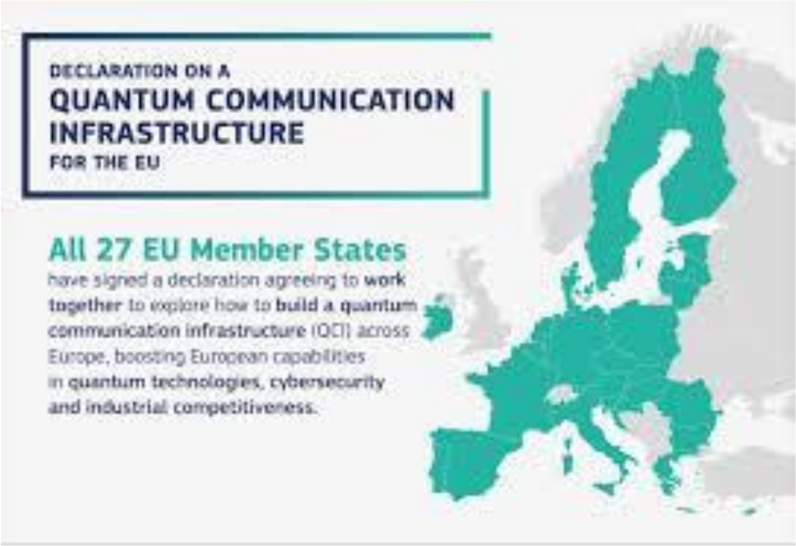


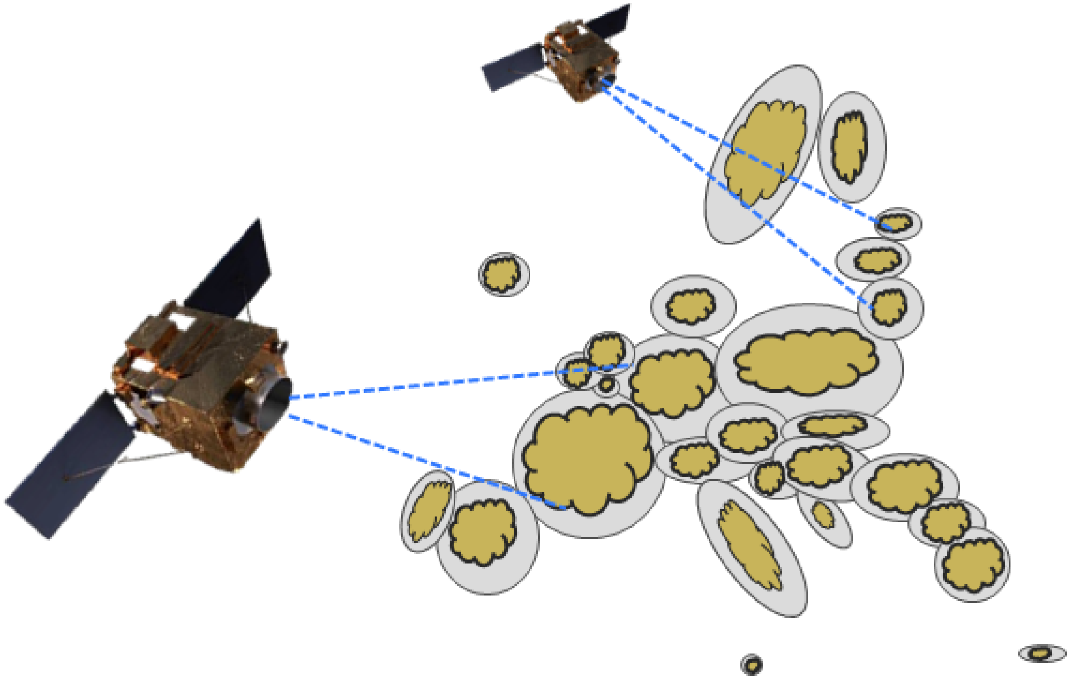
http://www.sci-news.com/physics/integrated-quantum-communication-network-china-09228.html

- Spanning Beijing to Shanghai (2000 km)
- Extended to 4600 km by use of free space QKD links
- Fibre losses limit distance between nodes to ~100 km
- Dedicated fibre network with **more than 30 trusted** nodes and 700 fibres

Quantum Communications: **EuroQCI**

European Quantum Communication Infrastructure

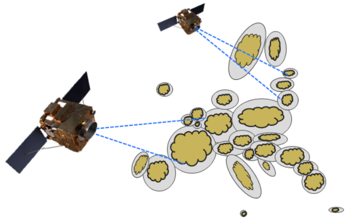




- ✓ **Sovereignty matters**
  - Hardware resources
  - Logical resources
- ✓ **National / international resources**
- ✓ **Security Level**
- ✓ **Interoperability**
  - Between National domains
  - Between terrestrial and space segment

AIRBUS

Airbus Quantum Communication footprint (EuroQCI – SAGA)



AnQUOR — EUROPEAN DEFENCE AGENCY — AIRBUS

2018 | 2019 | 2020 | 2021… | 2023.. | 2026 | 2027 | 2028 | 2034.. | Future

Preparatory activities EU funded research projects

QOSAC

Two Commercial concept studies
« High level Architecture »

AIRBUS

8tavo

Two studies
« Detailed Design »

AIRBUS

« QKD EU National Deployments » x26

AIRBUS

EuroQCI Coordination

PETRUS

AIRBUS *(partner)*

QKD Operational system

Quantum Internet

Terrestrial Quantum Communication Infrastructure

Space Quantum Communication Infrastructure

QKD Space backbone

SAGA I AIRBUS

SAGA II AIRBUS

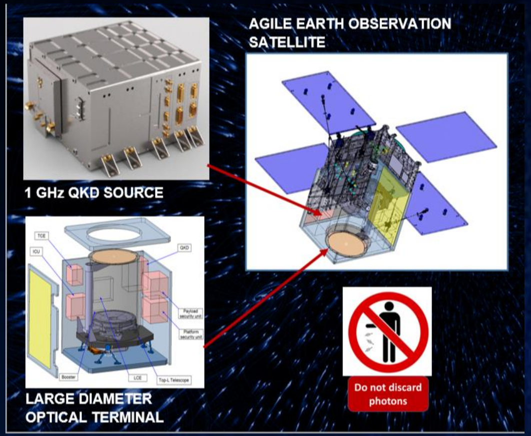
EAGLE 1 AIRBUS

Development of Optical Ground Station

IRIS2

Start of integration with EuroQCI

LaserPort - Optical Ground Station QKD – Final product



OGS at customer or secure hubs, to receive quantum keys from LEO satellites

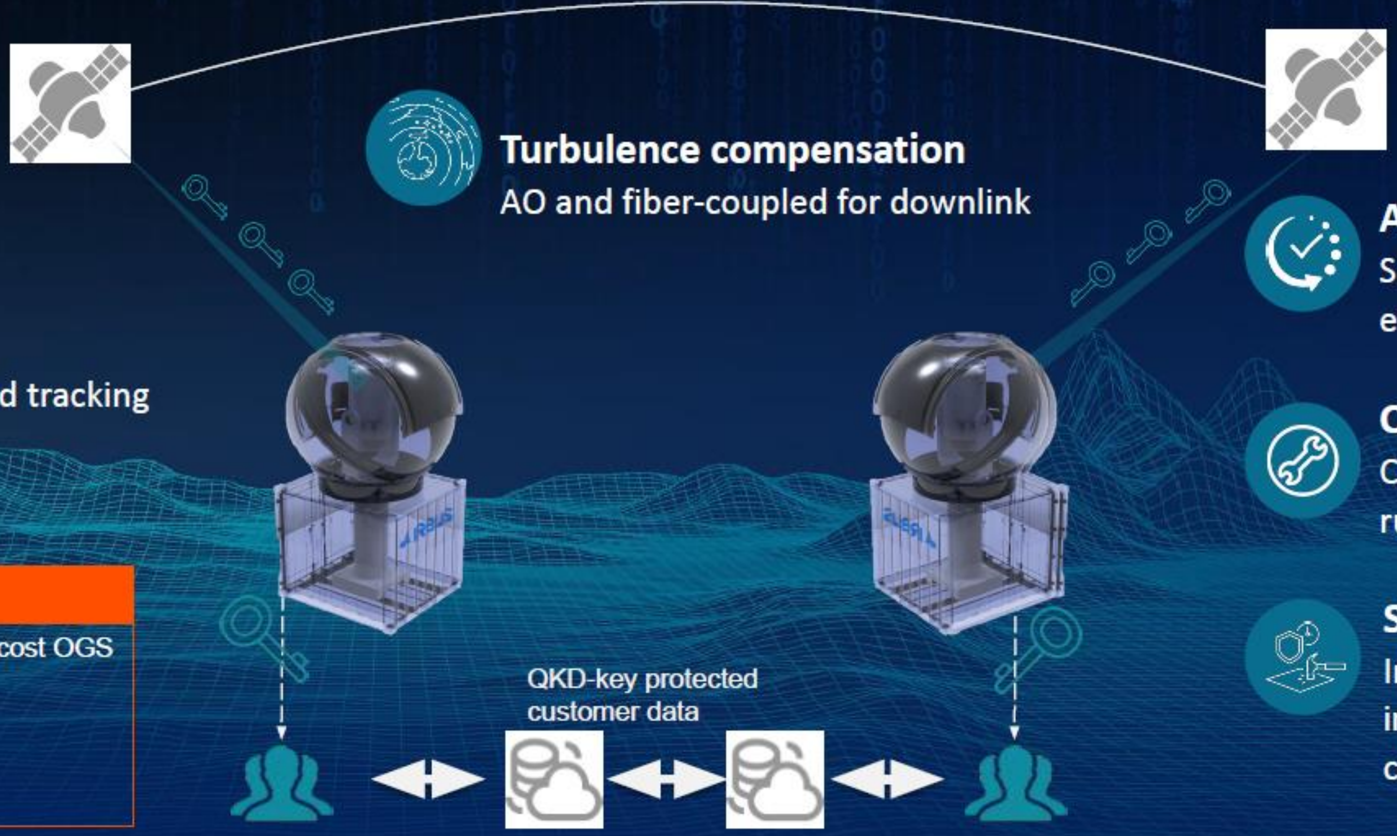
Turbulence compensation
AO and fiber-coupled for downlink

Pointing capacity
Full hemispherical
Robust Acquisition and tracking schemes

Availability
Support for broad environmental conditions

Characteristics
Compact, autonomous and ruggedized

Smart operations
Industrialized solution with integrated operations control software



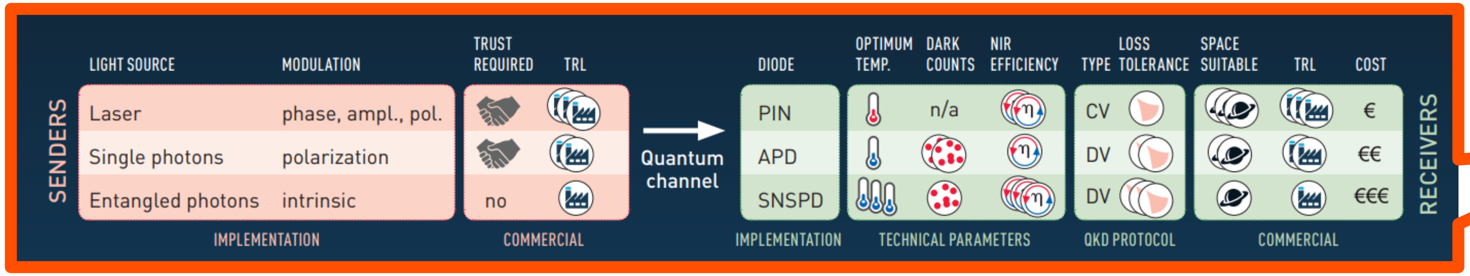
SOLUTIONS

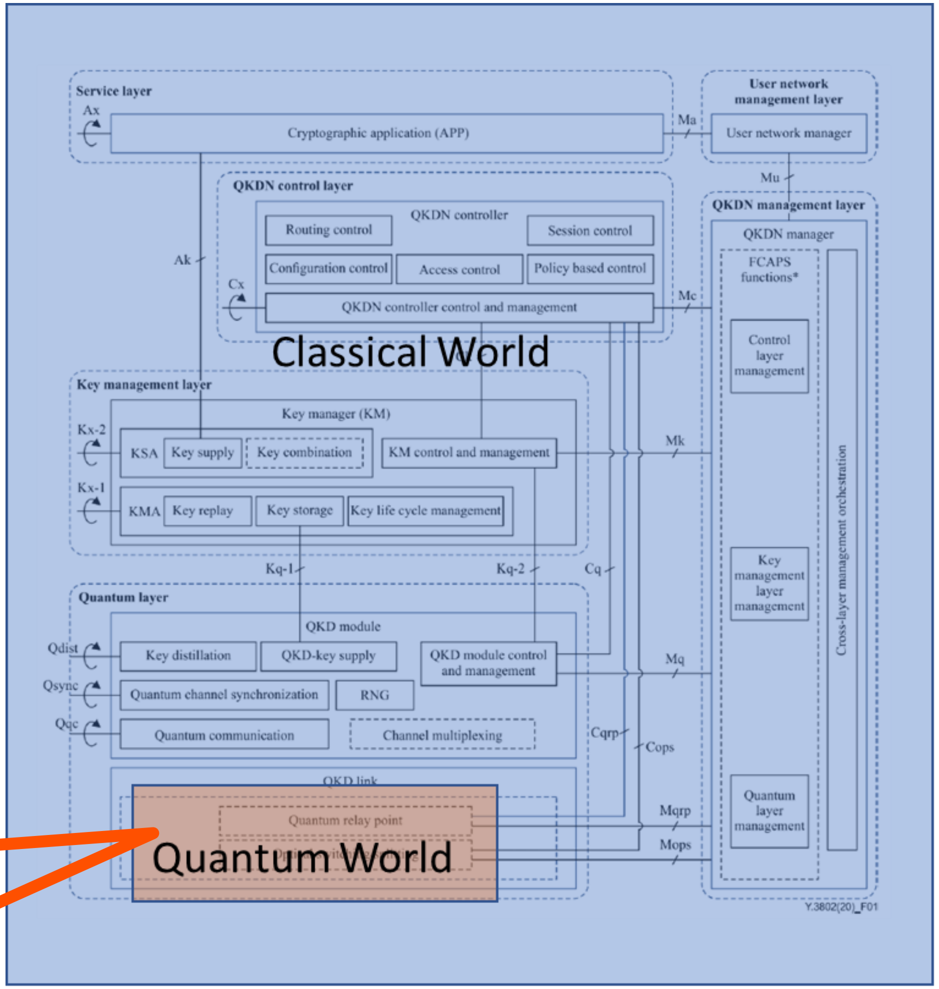
LaserPort LEO QKD: Low-complex, low-cost OGS for free space QKD (2027)

*Solution can be static or transportable

Quantum Communications: Interoperability

- System view of quantum-secure networks matters:
  - Quantum layer is relevant but is only a part of the overall system
  - Security matters: secure implementation, integration and interoperability is relevant
  - **PQC plays also an important role**
- Wide system design space exploration

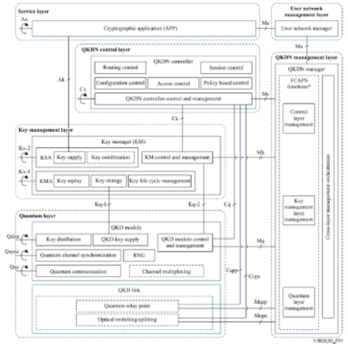


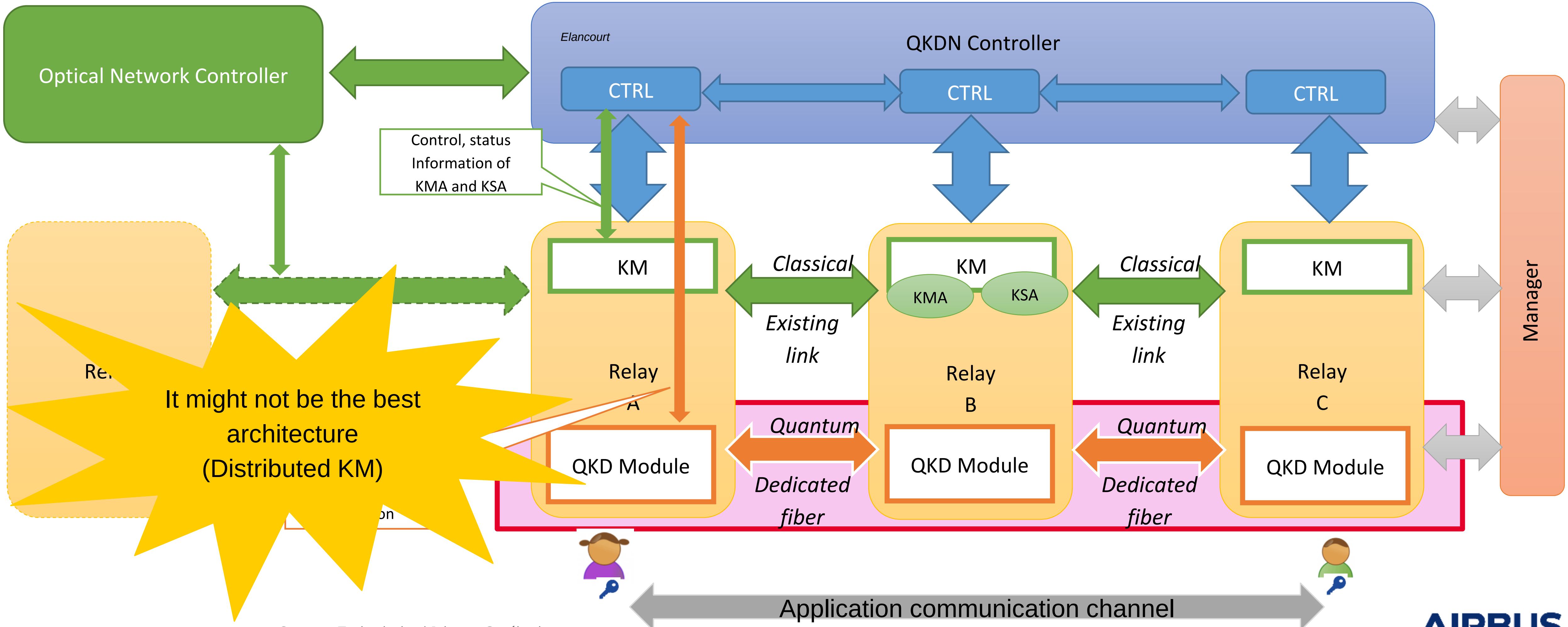


From ITU Y-3802

AIRBUS

An Example of a QCI architecture (high level view): Layered View (Note: Fully Distributed Key Management Layer)





AIRBUS

Looking to the future: Extended Space/Airborne QKD (HAPS and Drones)

NEEDS YOU!

Thank you

johanna.sepulveda@airbus.com

AIRBUS