Application Panel Quantum Communication

Introduction by the Chairs
2023-06-29

Dr. Felix Wissel

Prof. Andreas Tünnermann

Dr. Bettina Heim

WORLD OF QUANTUM

Deutscher Industrieverbund für Quantensicherheit

Agenda

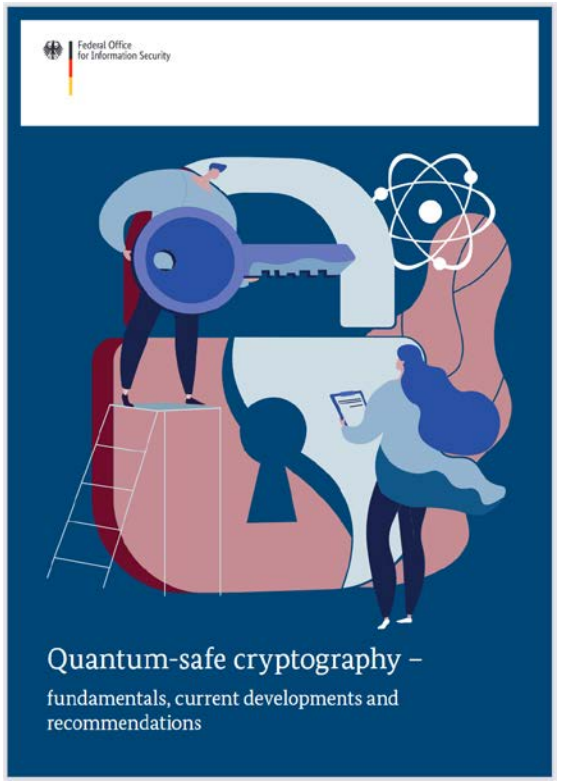
Time	Speaker and Affiliation	Talk Title
13:30 - 13:45	Dr. René Steiner, EC	How EuroQCI supports the uptake of QC in the EU
13:45 - 14:00	Niklas Lindman, ESA	SAGA 1st Generation - preparing for EuroQCI
14:00 - 14:15	Dr. Edeltraud Leibrock, Connected Innovations	How safe is safe? Developments and requirements from a Financial Services perspective
14:15 - 14:30	Dr. Marcell Gall, OHB System AG	QKD in Space – unique challenges in satellite-based Quantum Communication
14:30 - 14:45	Dr. Manfred Lochter, BSI	QKD and PQC from a security perspective
14:45 - 15:00	break	
15:00 - 15:15	Imran Khan, KEEQuant & Dr. Jasper Rödiger, R&S Cybersecurity	The SEQRET project within the Digital Europe Programme
15:15 - 15:30	Dr. Helmut Griesser, ADVA Network Security	QKD for the optical transport network
15:30 - 15:45	Marc Vanlerberghe, DT GBS Belgium	QKD@DT: Deutsche Telekom's Journey to Quantum Safeness
15:45 - 16:00	Dr. Alberto Comin	Airbus Group Satellite QKD Programs
16:00 - 16:15	Dr. Kevin Füchsel, Quantum Optics Jena	Quantum Key Distribution with Entangled Photons – How Noble Price Physics Revolutionize Cybersecurity
16:15 - 16:30	Dr. Emmanuel Fretel, Aurea Technology	Quantum safe communication, from Ground to Space!

Quantum Threat and Quantum Key Distribution - 101

- **“The quantum threat”**: Quantum computers will break today’s asymmetric algorithms
  - “Quantum computers will mainly present a danger to secure key exchange schemes.”
  - The threat is **real** and especially also **retroactively** wrt. already **stored** data
  - NSA operates data center, which stores encrypted communication
  - **Compromising** of **sensitive data**, which **needs long-term security**

- **Migration** to quantum-safe systems required:
  - Symmetric encryption
  - Quantum Key Distributions (QKD)
  - QC-resistent Algorithms (“Post-Quantum Crypto”)

“Quantum Safe Cryptography” by German BSI



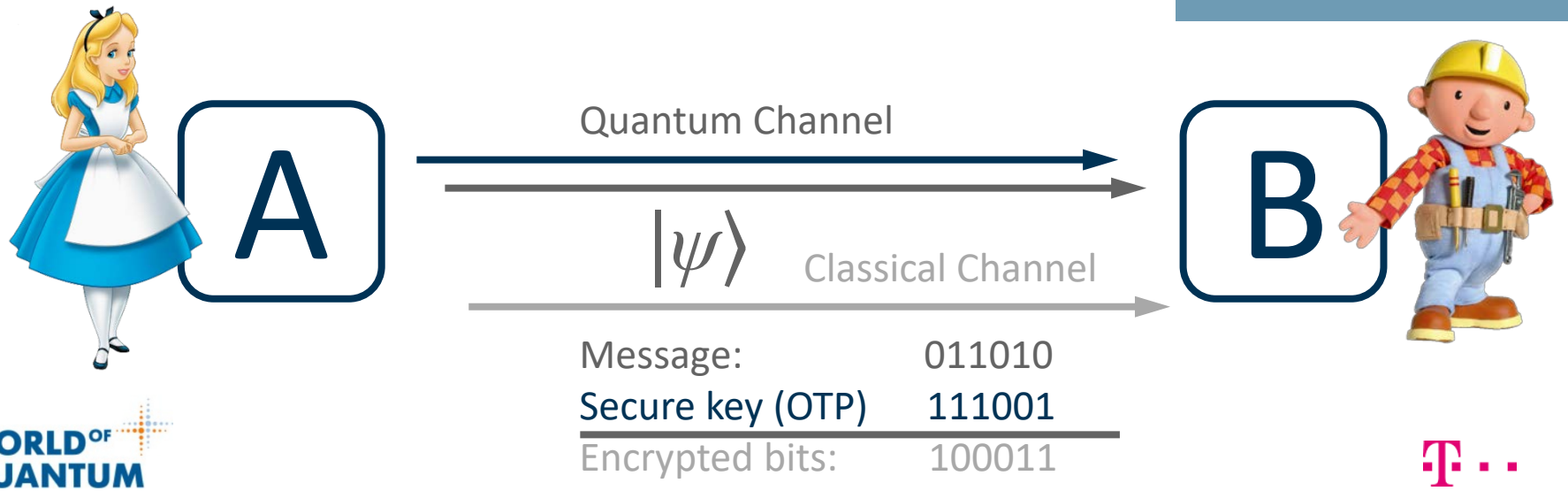
Quantum key distribution

A method to generate cryptographic keys exploiting quantum communication

- **Exchange** of **quantum states** between/to **A**lice & **B**ob via a quantum channel
- **A** randomly prepares & **B** randomly measures
- Authenticated classical channel needed for **classical post-processing**
  - Key sifting (basis matching)
  - Security estimation – determining and quantification of potential leakage to eavesdropper **E**ve
  - Error correction and privacy amplification
    → identical and reduced cryptographic key, shared only by **A** & **B**

- **QKD** generated keys to be used in Key Management Systems in **Hybrid Solutions**
- Combination with PQC, Symmetrical Encryption
- Various crypto sources combined by Key Derivation Functions

QKD enables **information-theoretic P2P key exchange** where its security…
- is based on **quantum physics**
- can be proven **without restrictions** on eavesdropper



Alice Character by Walt Disney, Bob the Builder character by Keith Chapman

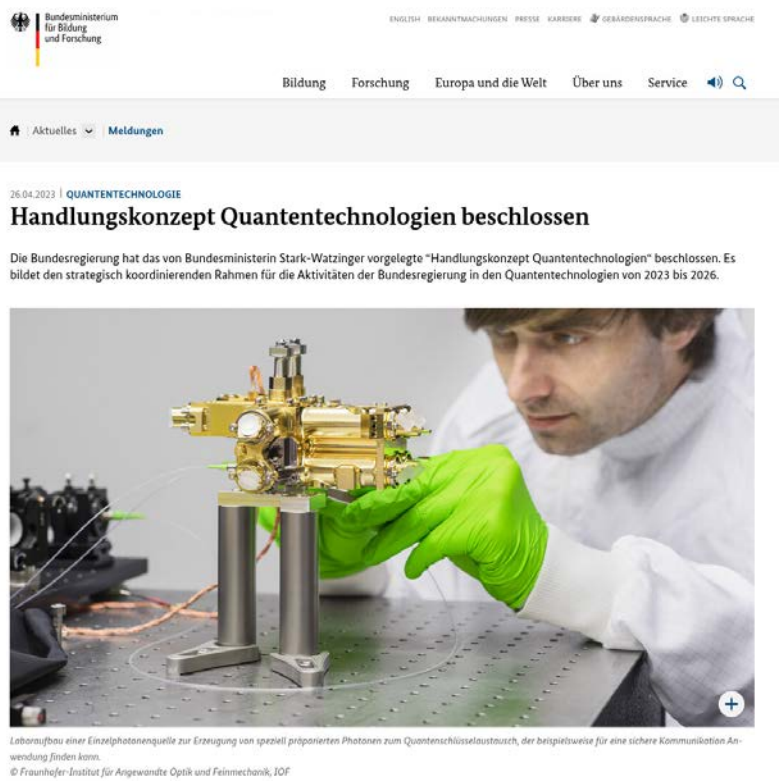
Quantum Technologies in Germany

Federal “Handlungskonzept” quantum technologies

- **Strategic framework** for the **German government's activities** in quantum technologies
- **Interdepartmental concept**,
  comprising various departments of the federal German government
- Developed under the **leadership of BMBF**
- Approved in April 2023

- Divided into three fields of action:
  - development of **application-ready products**
  - targeted **technology development**
  - promoting a **strong ecosystem**

→ Development & coordination of various funding programs focusing on
- quantum computing and quantum simulation,
- quantum communication and post-quantum cryptography,
- quantum sensing and quantum metrology



Laboraufbau einer Einzelphotonenquelle zur Erzeugung von speziell präparierten Photonen zum Quantenschlüsselaustausch, der beispielsweise für eine sichere Kommunikation Anwendung finden kann.
© Fraunhofer-Institut für Angewandte Optik und Feinmechanik, IOF

→ Total Budget 3 B€ from 2023 - 2026 (2.18 B€ + 850 M€ contributed by the science organizations)

Quantum Communication in Germany

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SQuaD
Schirmprojekt Quantenkommunikation Deutschland

SQuaD:

- Consortium with excellent and complementary expertise in Quantum Communication

Central goals:

- Support the coherent development of a Quantum Communication Ecosystem in Germany
- Secure a strong role for Germany and Europe in Quantum Communication Commercialization
- Leverage synergies, avoid duplications
- Optimal use of resources to ensure competitive position in the international environment
- Support German technological sovereignty

QuNET – Quantum Technologies for Secure Communication

WWW.QUNET-INITIATIVE.DE

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

- A joint national initiative of the Federal Ministry of Education and Research, the Fraunhofer Society , the German Aerospace Center, the Friedrich Alexander University, and the Max Planck Society (Core institutes: DLR-IKN, Fraunhofer IOF & HHI, FAU, MPL)

DLR · Fraunhofer · FAU Friedrich-Alexander-Universität Erlangen-Nürnberg

- Cooperation with the German Federal Office for Information Security (BSI), combination with post-quantum cryptography methods (PQC)
- 7-year term (2019 - 2026), approx. €125 million project volume
- Goals:
  - Enabling realistic application scenarios
  - Transfer to industry
  - Preparation of certification, standardization & EuroQCI
  - Demonstration of core components in key experiments
  - Roadmap process & agile project management
  - Value chain from components to systems to network implementations

WORLD OF QUANTUM · Fraunhofer IOF · OHB

QKD in Germany- DIVQSec

German Industry Federation for Quantum Security

Deutscher Industrieverbund für Quantensicherheit

Goal:

- Industrialized solutions for quantum safe communication
- Guarantied technology sovereignty

Way of Working:

- Communication Platform and Shaping of Ecosystem
- Consolidate Interests of members and common representation

Interfaces:

- Federal and Europe Politics
- Further interests groups within Europe
- Fundamental research
- Public

Elected Speakers:

- Norbert M.K. Lemke, OHB
- Imran Khan, KEEQuant

ADVA

DB Systel

IABG

KEEQUANT

OHB

QuantiCor

QUANTUM OPTICS JENA

ROHDE&SCHWARZ

qutools

TESAT

TOPTICA

evolution

WORLD OF QUANTUM

QKD in Europe

Basic Research

- **Quantum Flagship:**
  - The 3rd large-scale research and innovation initiative funded by the European Commission
  - Started in October 2018, running time 10years, overall budget 1 Billion €
  - To bring together research institutions, industry and public funders, consolidating and expanding European scientific leadership and excellence
- First ramp-up phase 2018 – 2022
  - CiViQ – Continuous Variable QKD
  - QRANGE – Quantum Random Number Generator
  - (OpenQKD)
- Second phase 2023 -2027
  - QSNP – Quantum Secure Network Partnership
  - QIA – Quantum Internet Alliance

QKD in Europe

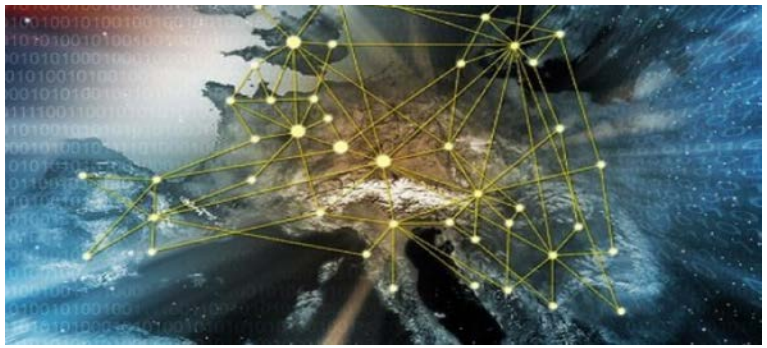
EuroQCI

EuroQCI

- An **integrated satellite** and **terrestrial** system spanning the whole EU for **ultra-secure exchange** of **cryptographic keys** (Quantum Key Distribution)
- **Quantum communication infrastructure (QCI)** is part of the **European Cybersecurity Strategy** and is to be **integrated** in the new **Secure Space Connectivity initiative "IRIS²"**

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



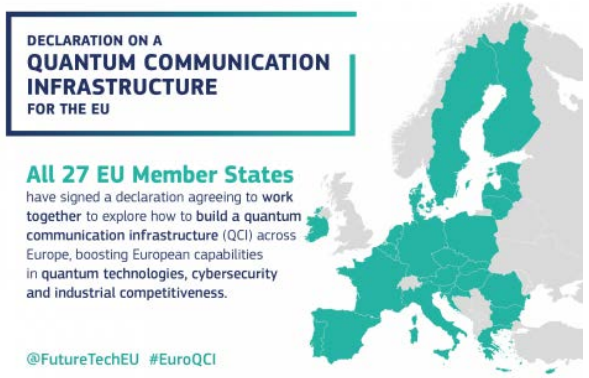
Source: European Commission

IRIS² ⊇ EuroQCI = SpaceQCI + TerrQCI

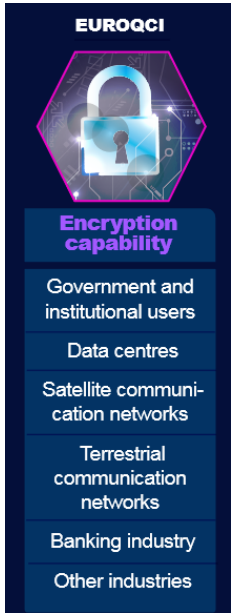
Apr. 2019: Collaboration agreement between **EC** and **ESA** for development and deployment within the next ten years of a **EU Quantum Communication Infrastructure (QCI)**[1]

Jul. 2021: **All EU Member States** committed to building the EuroQCI[2]

Nov. 2022: EuroQCI **to be integrated into IRIS²** (EU budget of €2.4 billion), the new EU **Infrastructure for Resilience, Interconnection & Security by Satellites**[4]



- IRIS² & EuroQCI **overall system** and **terrestrial component** under EC responsibility
- **Space-based component SpaceQCI** under **ESA** responsibility
- EuroQCI to provide **quantum cryptographic keys** to protect communication systems of European institutions and critical infrastructure → **additional layer of security** based on quantum physics
- EuroQCI as a fully **operational system** based on EU user requirements

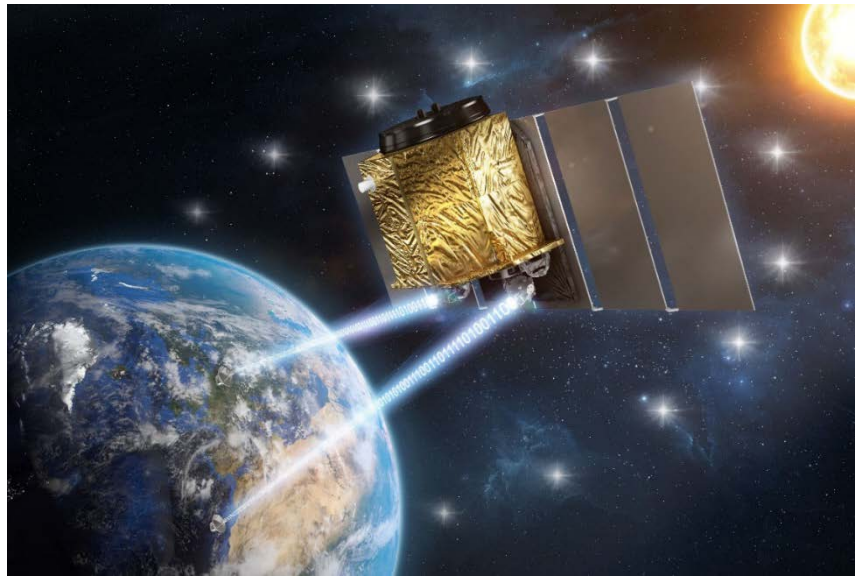


1 https://artes.esa.int/news/esa-and-ec-sign-agreement-european-quantum-communications
2 https://digital-strategy.ec.europa.eu/en/news/all-member-states-now-committed-building-eu-quantum-communication-infrastructure
3 https://digital-strategy.ec.europa.eu/en/news/austria-bulgaria-denmark-and-romania-join-initiative-explore-quantum- communication-Europe
4 https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_6999 & https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-programme/iriss_en

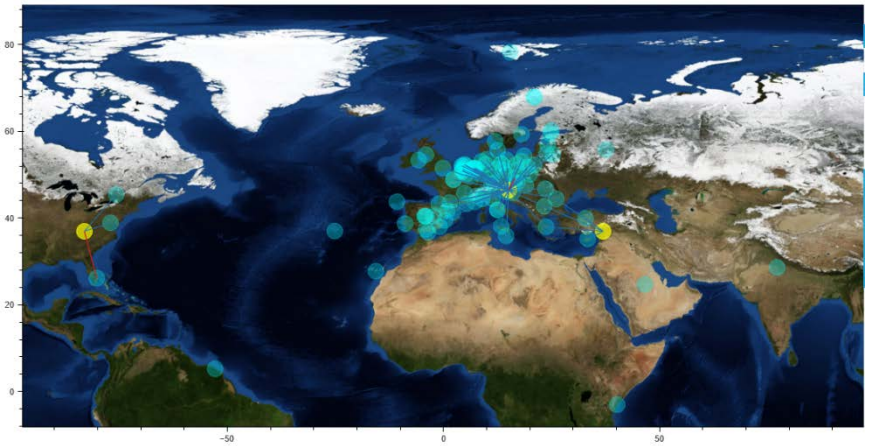
SAGA – Secure And cryptoGrAphic mission

EuroQCI space-based component

- IRIS² to **gradually integrate EuroQCI/SAGA** into **governmental services**
- For EuroQCI being fully functional
  → **SAGA early service validation required**: SAGA 1st Generation **(S1G): 1 satellite, LEO, focus on P&M** service
- Deployment within the next 10 years
- 3 parallel SAGA Phase A studies from 01/2021 – 07/2022
  Strong interaction with EC EuroQCI and ESSCS studies
- 2 parallel Phase B1 studies for S1G started 01/2023
  - one for Airbus + one for OHB/TAS
- Next Step: security-related Technology Maturation Activity



Artist's Impression of the SAGA Spacecraft, here with two optical terminals/QKD links



(Figure only for illustrative purposes – does not reflect the real system design)

QKD in Europe

Digital Europe Programme

DIGITAL-2021-QCI-01-INDUSTRIAL

- Create a European Industrial Ecosystem for secure QCI technologies and systems
  - eCausis
  - Equo
  - MDI Queen
  - Qkiss
  - Quarter
  - Seqret

DIGITAL-2021-QCI-01-DEPLOY-NATIONAL

- Deploying advanced national QCI systems and networks
  - First deployed QKD networks integrated and operating with existing communication networks in several Member States

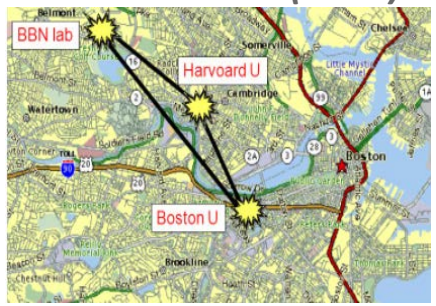
DIGITAL-2021-QCI-01-EUROQCI-QKD

- Coordinate the first deployment of national EuroQCI project and prepare the large-scale QKD testing and certification infrastructure

QKD around the World

QKD Network Demonstrators

DARPA (2002)



SECOQC (2008)

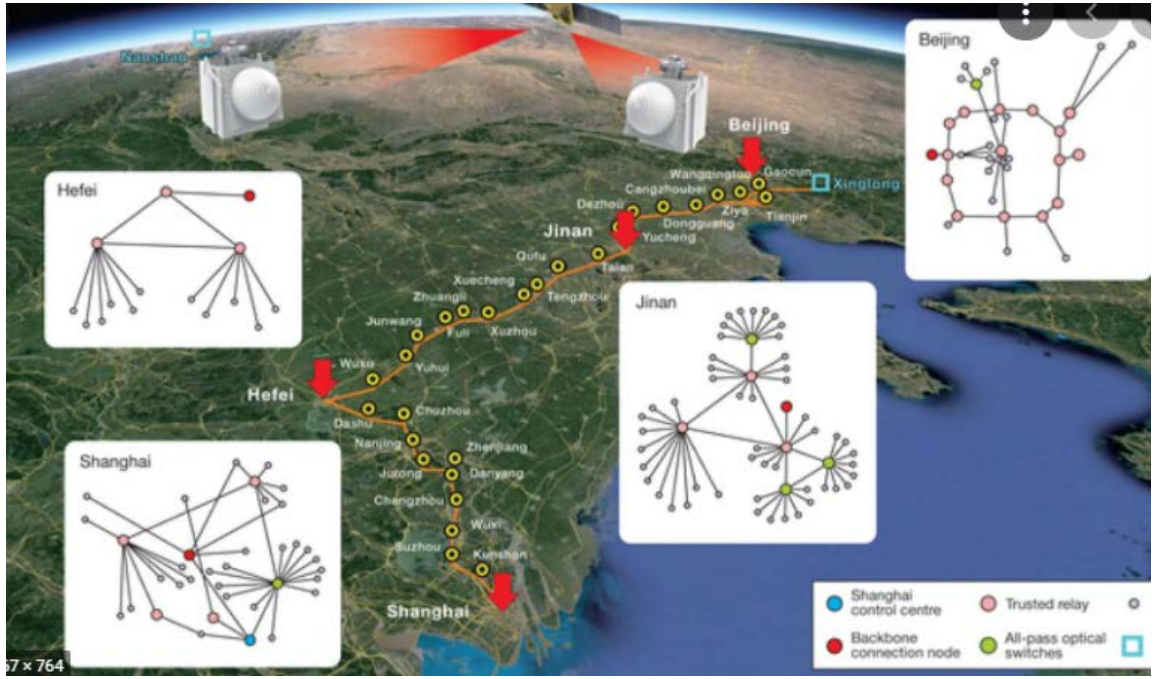
TOKYO (2009)

SOUTH KOREA (2015, 2017, 2020)

ITALY (2018)

CAMBRIDGE (2019)

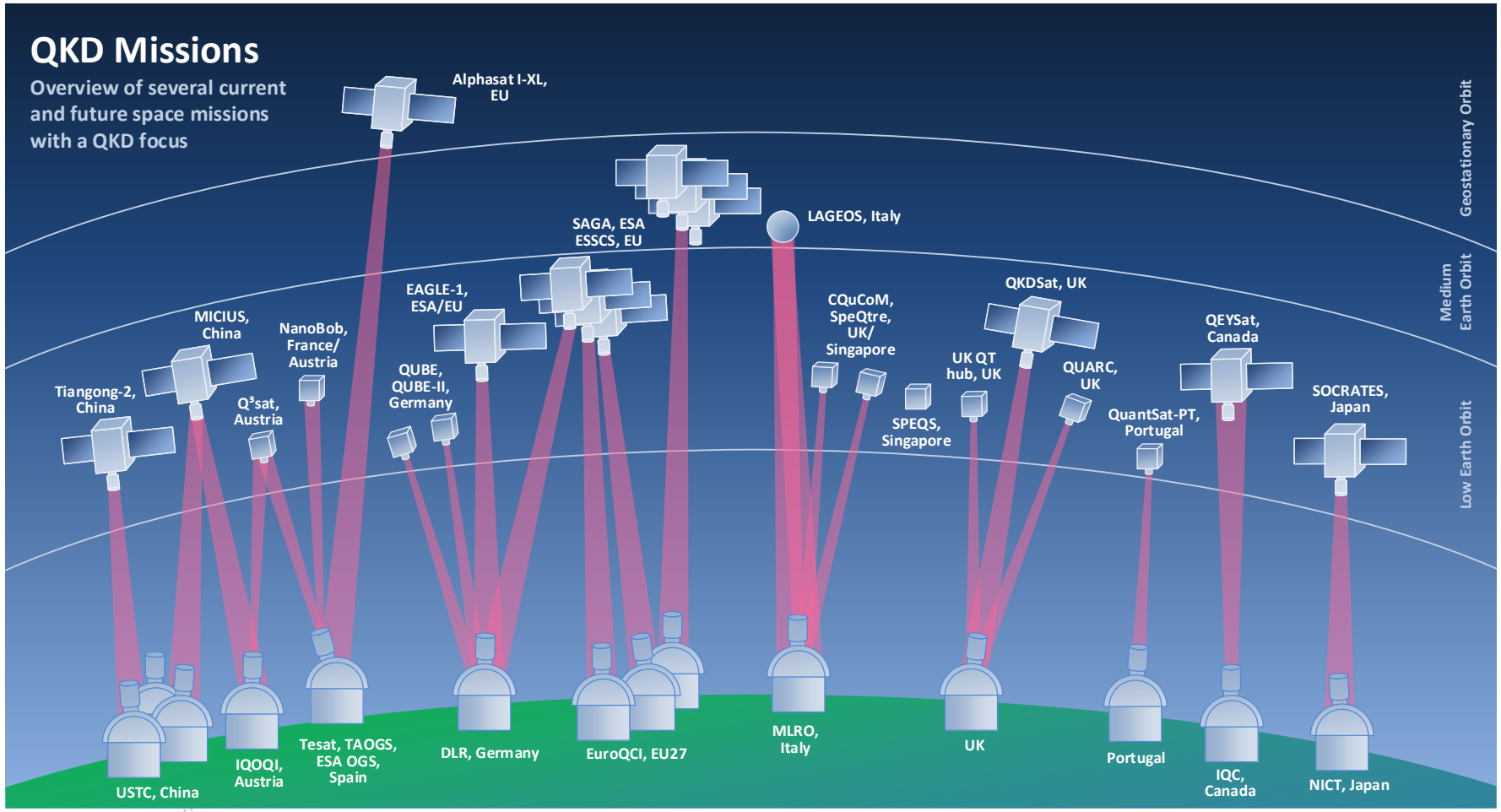
Chinese QKD Network



- 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

QKD around the World

Space-Based Missions



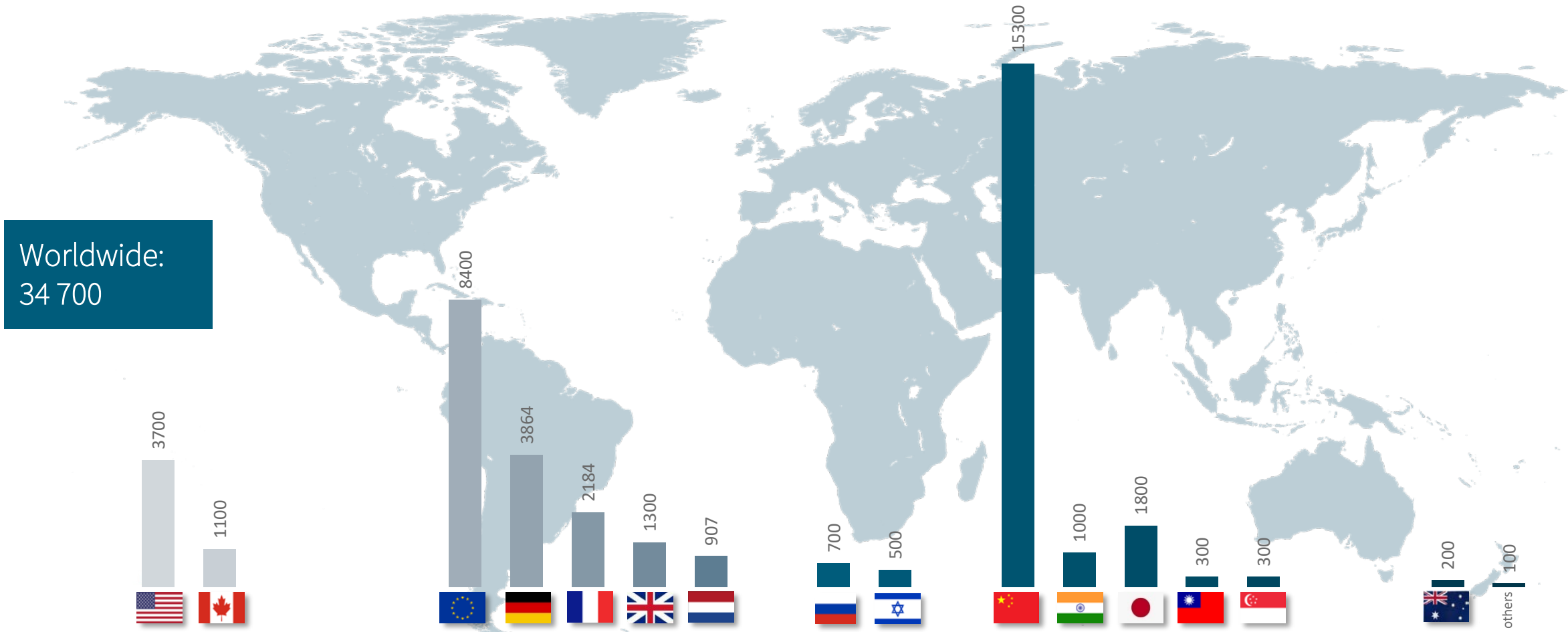
Source:

Space-based Quantum Communication, Luft- und Raumfahrt, Issue 2 / 2022
Norbert M.K. Lemke, Bettina Heim, Imran Khan, Thomas Sichert

Public Investment into Quantum

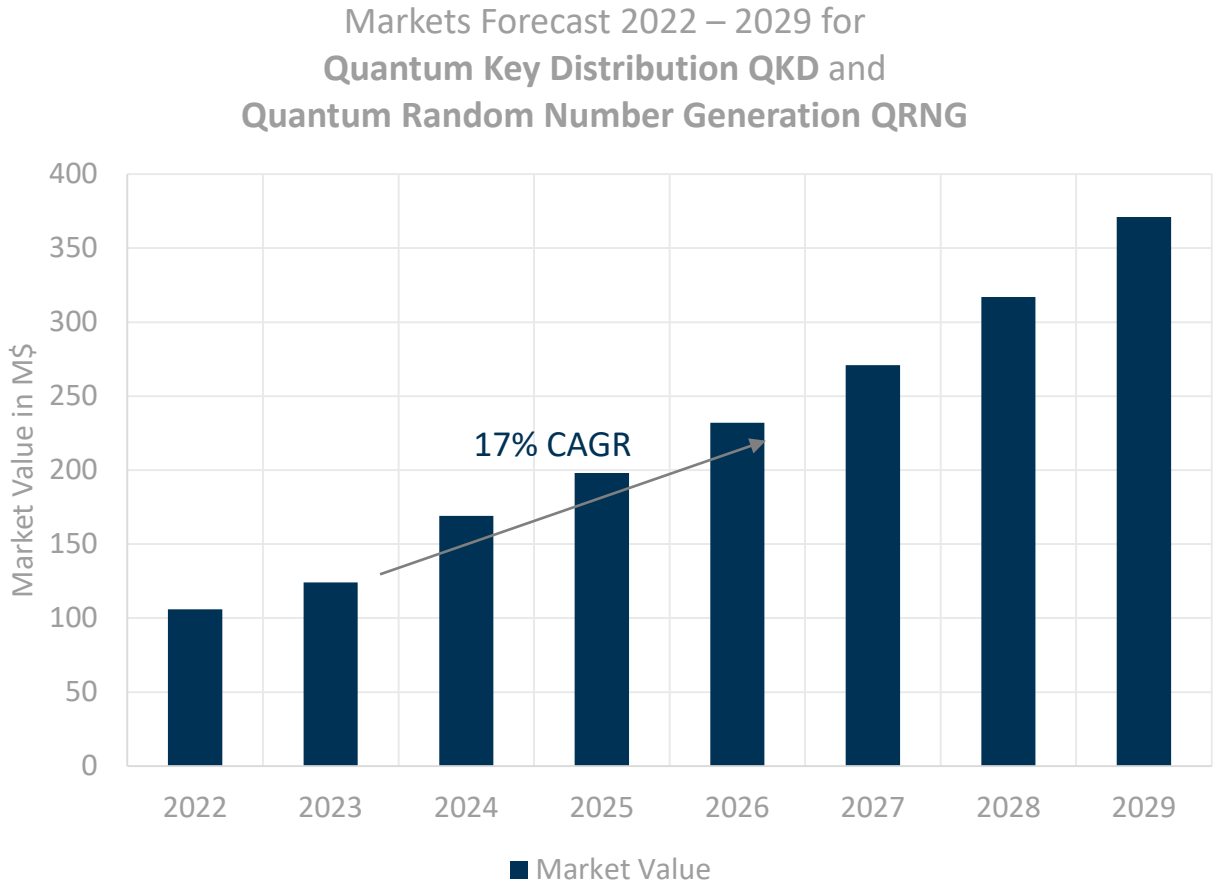
Worldwide, in $ million

Source: McKinsey & Company: Quantum Technology Monitor April 2023



Quantum Communication Market Developments

- Main applications for quantum communication
  - Securing mobile & payment systems
  - Connecting data centers
  - Enabling telecom & services
  - Protecting civil government
  - Encryption of military communications



Source: Yole: Quantum Technologies 2023, Market and Technology Trends

Challenges & Outlook

What is needed? What is done

- Standardisation & Certification
- EU-27 independent supply chains
- End-2-End service definition
- Customer management and ‘Triple A’ (Authentication, Authorization, Accounting)
- Integration into existing infrastructure (management & control plane, Operational Support Systems (OSS))
- Governance structures
- Harmonisation of different activities (EC, ESA, Member States), schedules and roadmaps

- March ’23: CEN/CENELEC → Joint Technical Committee 22 on Quantum Technology
- Each day now: Digital Europe Programme → Testing & Validation Infrastructure
- Oct ’23 ETSI QKD ISG: CC:2022/CEM:2022 Protection Profile for a pair of P&M QKD Modules→ certification expected
- Somewhen later: Connecting Europe Facilities (CEF) → Cross Border Connections

Contacts

Your chairs

OHB System AG
Manfred-Fuchs-Straße 1
82234 Weßling / Oberpfaffenhofen
Germany

Dr. Bettina HEIM
bettina.heim@ohb.de
Phone +49 8153 4002-298

Deutsche Telekom Technik GmbH
Ida-Rhodes Straße 2
64295 Darmstadt
Germany

Dr. Felix WISSEL
felix.wissel@telekom.de
Phone +49 6151 5836016