



# Putting quantum communications into action

Jörg-Peter Elbers, ADVA

NetSys 2021, ZdN - Advanced networking technologies

# AGENDA

1. The wonderful quantum world
2. Quantum-safe communications
3. Quantum key distribution
4. Towards the Quantum Internet
5. Conclusions





# The wonderful quantum world



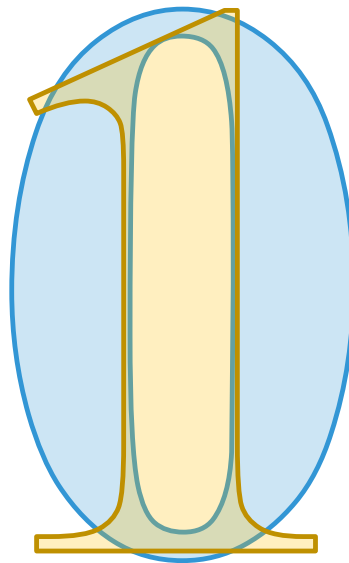
# The power of quantum computing

Classical bit

Quantum bit (qubit)



or

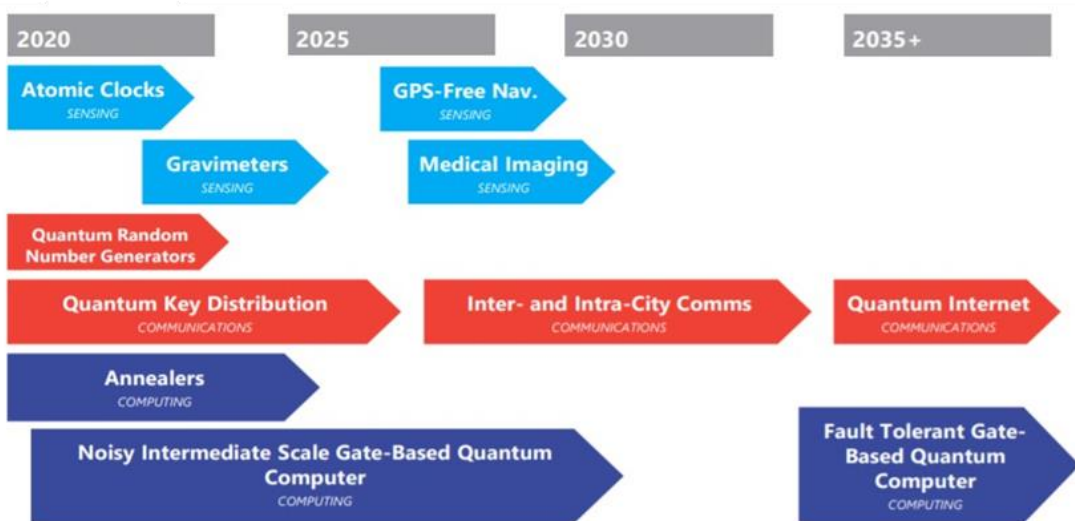


A quantum computer with 50 qubits can process  $2^{50} = 1.125.899.906.842.624$  states simultaneously

# Quantum technologies are getting much attention

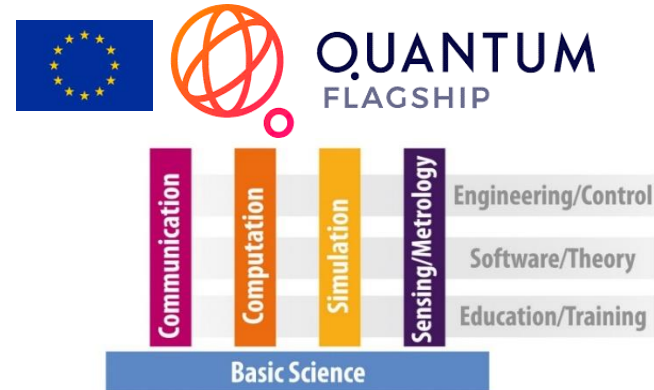


## Quantum Technologies Timeline



\*Chevron placement represents anticipated start date of commercialization  
Source: Expert interviews, Newry analysis

[https://www.osa.org/en-us/industry/industry\\_intelligence/oidaroadmap/](https://www.osa.org/en-us/industry/industry_intelligence/oidaroadmap/)



BEAUFTRAGT VOM



Bundesministerium  
für Bildung  
und Forschung



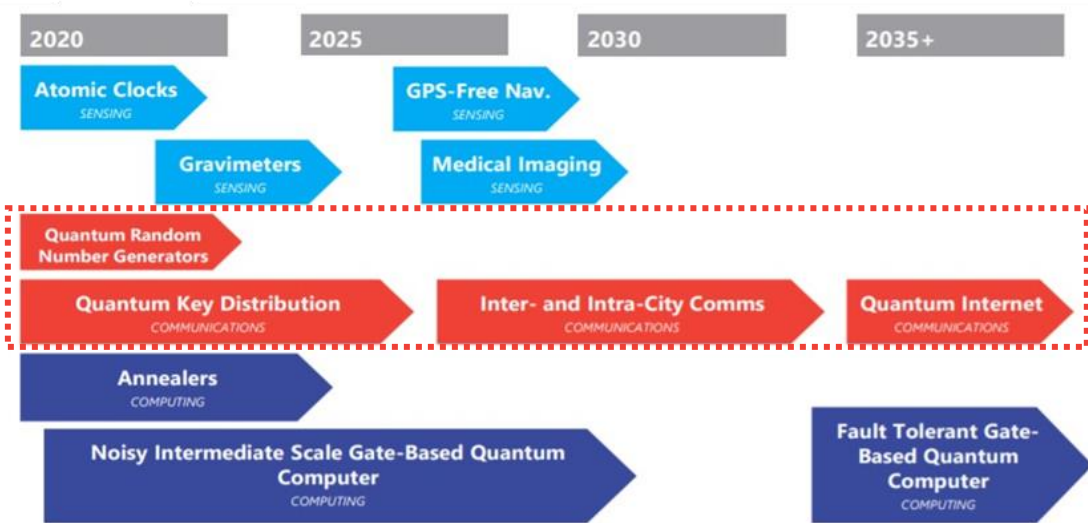
quanten  
technologien

Billions of Euros are being invested in a global quantum race

# Quantum communication is one of the applications



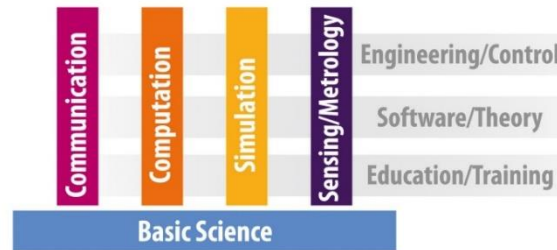
## Quantum Technologies Timeline



\*Chevron placement represents anticipated start date of commercialization  
Source: Expert interviews, Newmy analysis



QUANTUM FLAGSHIP



BEAUFTRAGT VOM



Bundesministerium für Bildung und Forschung



quanten technologien

Near term market potential for QRNGs and QKD



# Quantum-safe communications

# Encryption protects sensitive data ...



**Encryption works.**

**Properly implemented strong crypto systems are  
one of the few things that you can rely on.**

*Edward Snowden*

Freedom of the Press Foundation, [Edward-Snowden-FOPF-2014](#), [CC BY 4.0](#)

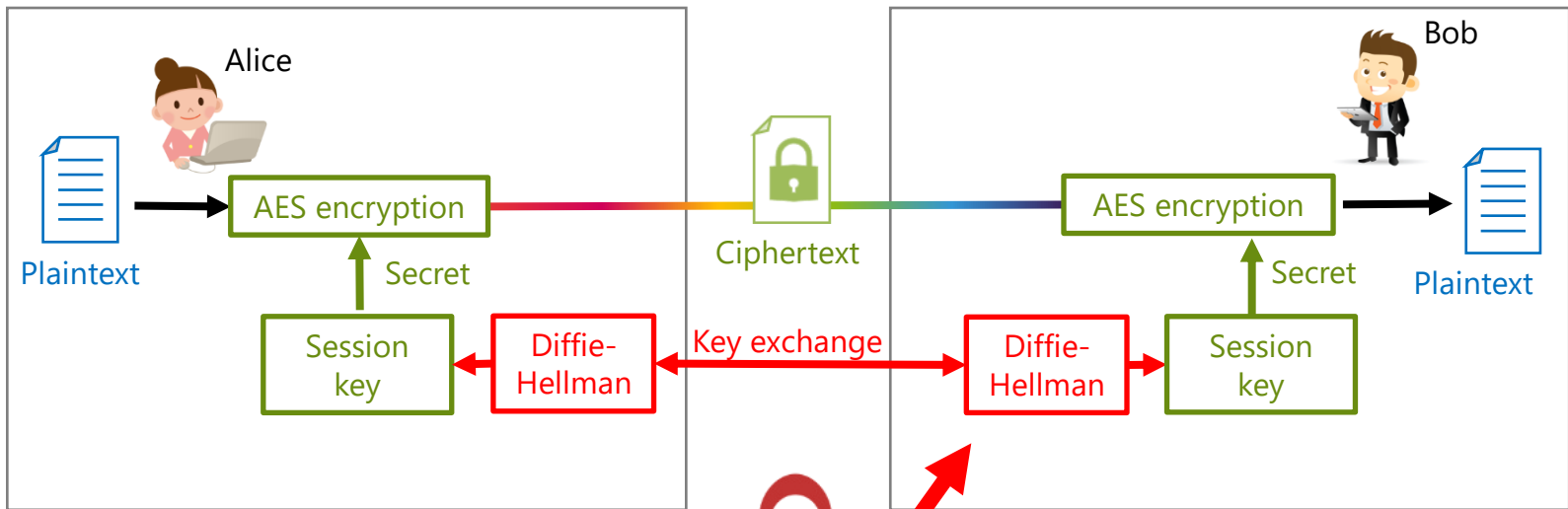


# ... but can be broken by large quantum computers



Attack scenario: Store now, decrypt later

# The classical key exchange is the weak link



AES: Advanced Encryption System

Most popular public-key algorithms can be broken by a quantum computer

New quantum-safe solutions are needed



# Quantum-safe key exchange methods

## Two lines of defense

### Post-quantum cryptography (PQC)

- Is based on hardened algorithms
- Works with any communication channel
- Requires endpoint access on protocol level
- Is independent of optical link parameters

### Quantum key distribution (QKD)

- Is based on laws of quantum physics
- Needs optical fiber or free-space media
- Requires access to physical infrastructure
- Depends on optical link parameters

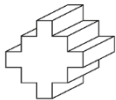
First line of defense

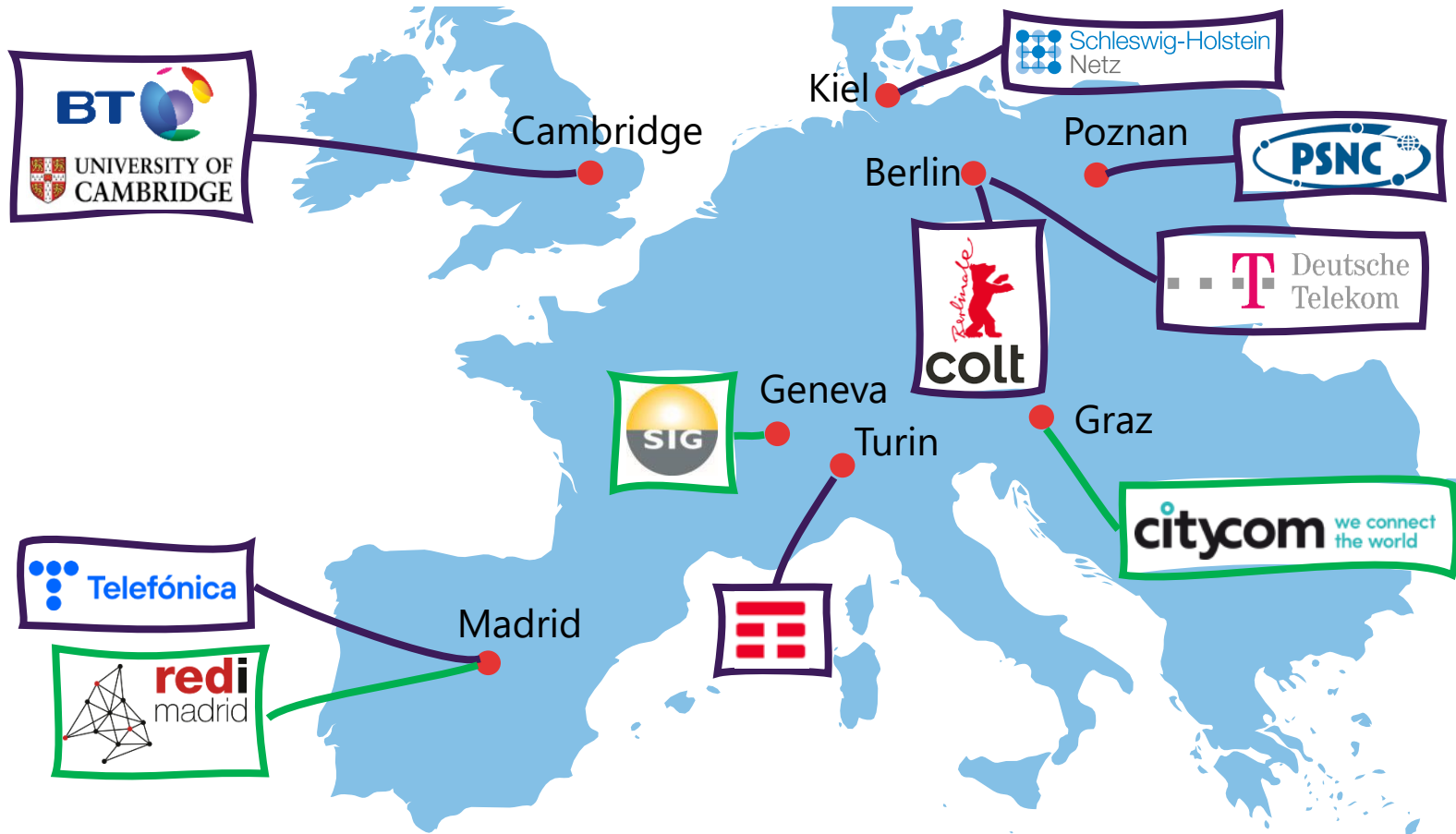
Additional protection



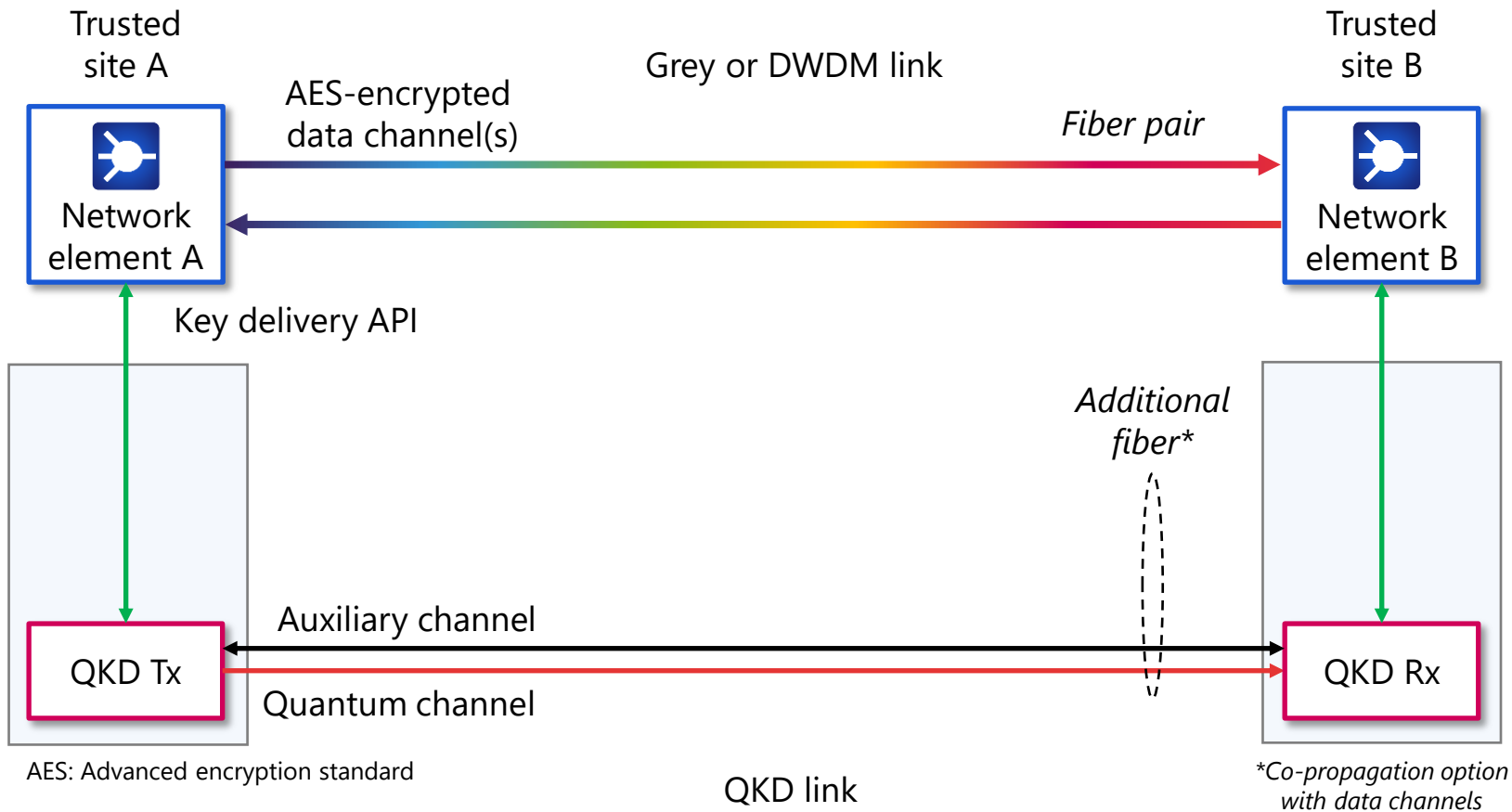
# Quantum key distribution

# ADVA: Enabling QKD deployments

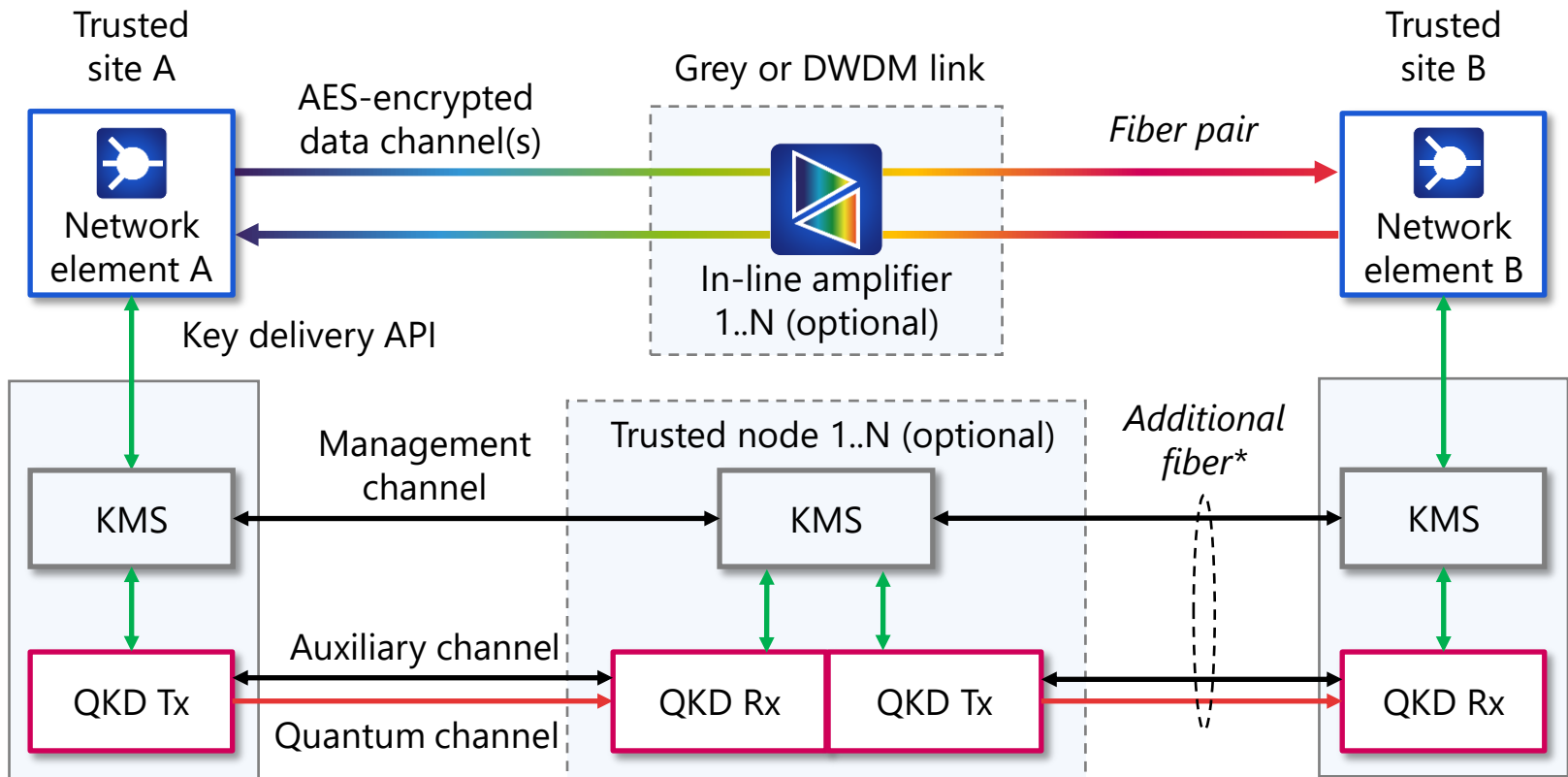
OPEN  QKD



# QKD is part of a larger network encryption solution ...



# ... and creates dependencies important to understand

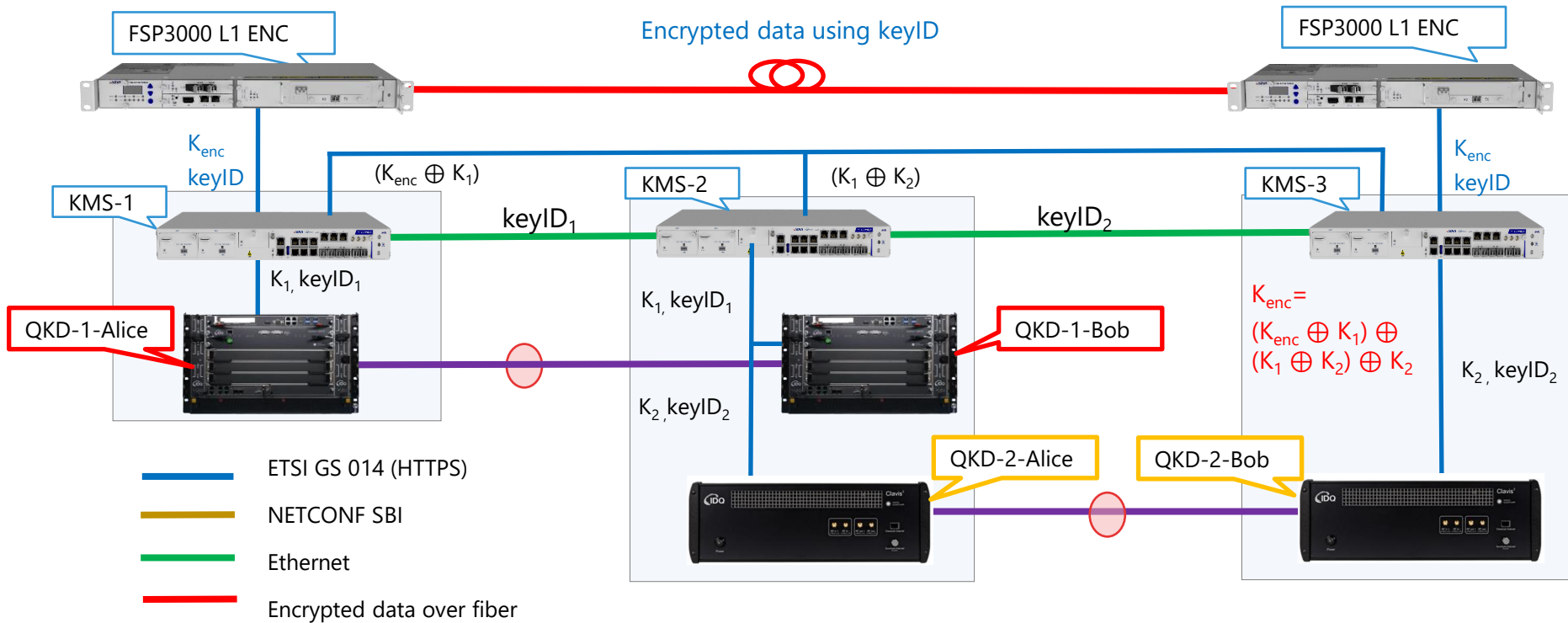


AES: Advanced encryption standard  
 KMS: Key management system

QKD link

\*Co-propagation option with data channels

# Trusted node QKD demo

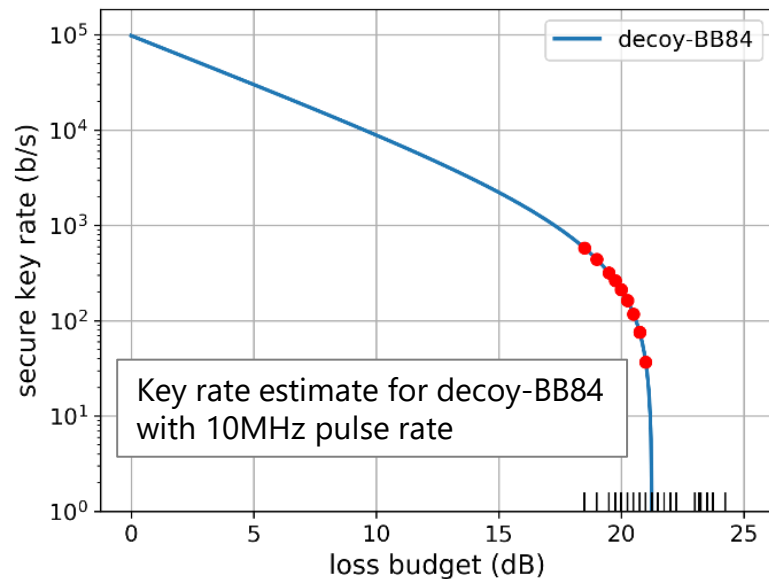
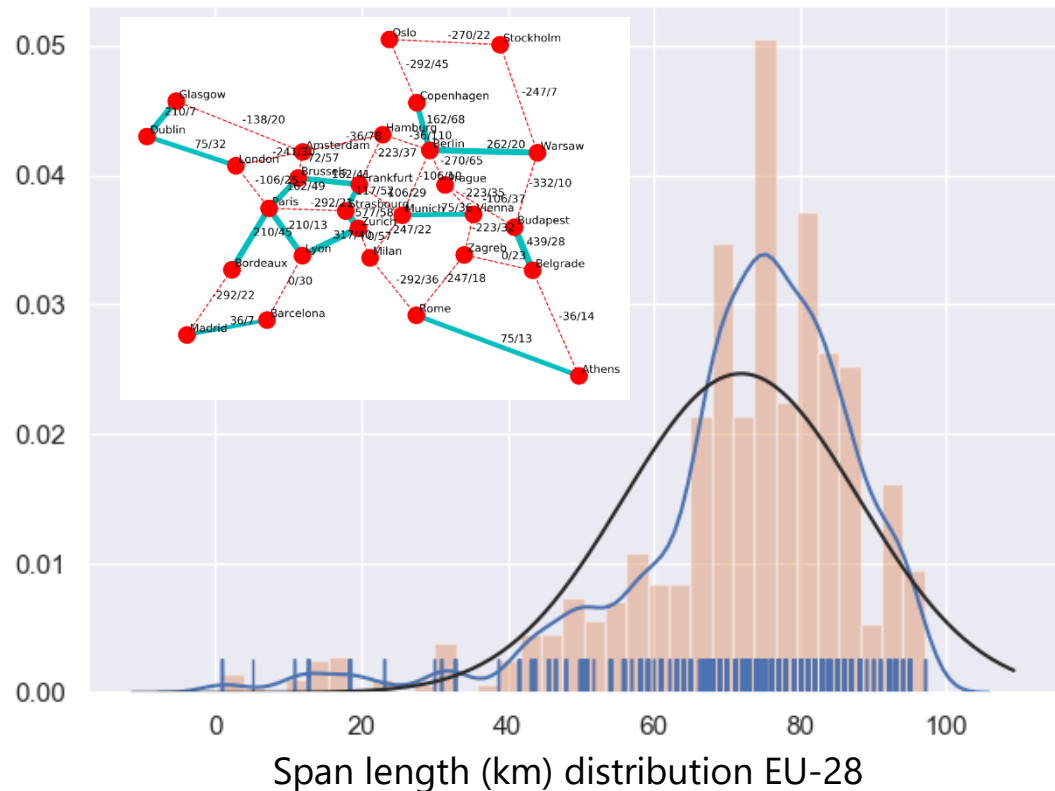






# Towards the Quantum Internet

# From p2p QKD-links to an EU-wide deployment



Nobel network model with typical span length distribution and 0.25dB/km. Ref: T. Szymanski, "Maximum Flow Minimum Energy Routing in Exascale Cloud Computing Systems," 2013

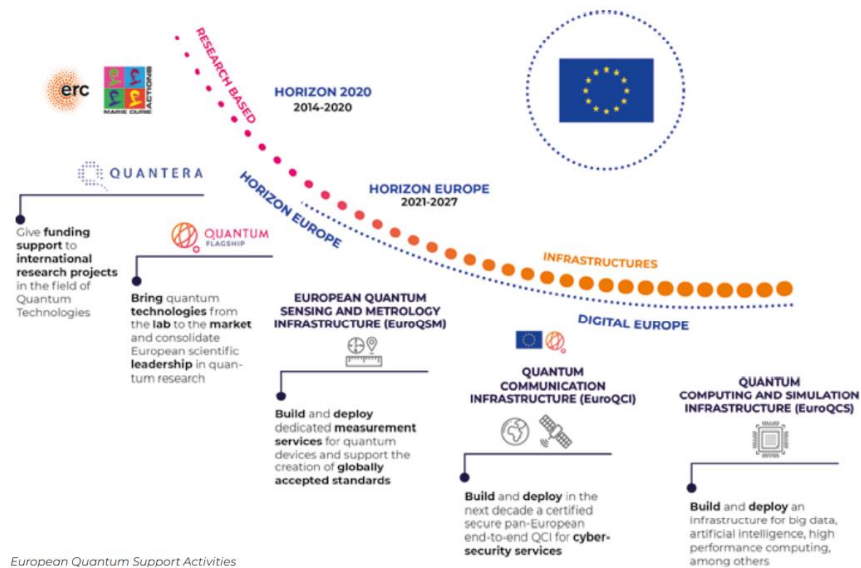
# Euro-QCI as stepping stone to the Quantum Internet

**DECLARATION ON A  
QUANTUM COMMUNICATION  
INFRASTRUCTURE  
FOR THE EU**

## All 27 EU Member States

have signed a declaration agreeing to work together to explore how to build a quantum communication infrastructure (QCI) across Europe, boosting European capabilities in quantum technologies, cybersecurity and industrial competitiveness.

@FutureTechEU #EuroQCI



[https://qt.eu/app/uploads/2020/04/Strategic\\_Research-Agenda\\_d\\_FINAL.pdf](https://qt.eu/app/uploads/2020/04/Strategic_Research-Agenda_d_FINAL.pdf)

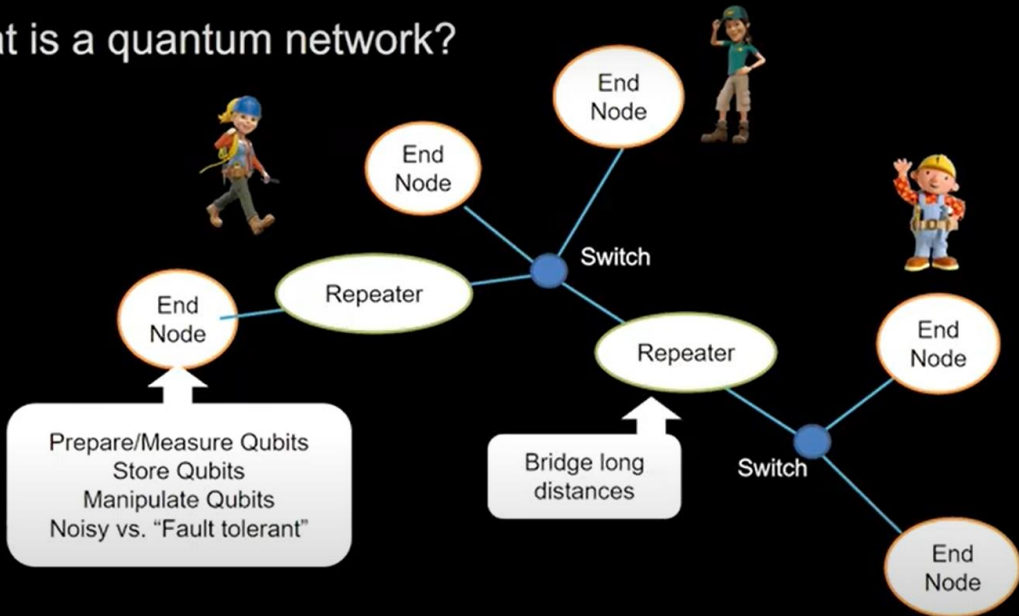
Euro-QCI is planned to be fully operational by 2027

# The Quantum Internet vision



DLS: Stephanie Wehner - Towards a Blueprint for a Quantum Internet

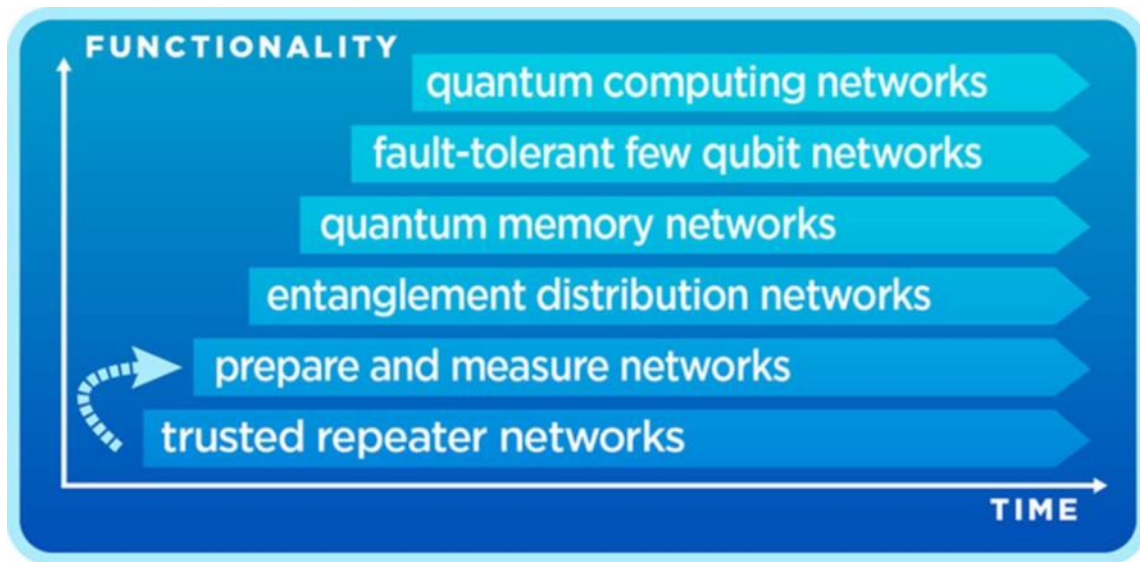
## What is a quantum network?



<https://www.youtube.com/watch?v=ig6TqDChnWI>

Enabling worldwide quantum communication via fiber or satellite

# Stages of the Quantum Internet



S. Wehner et al., Science 362, eaam9288 (2018). DOI: 10.1126/science.aam9288

Quantum repeaters are necessary for end-to-end Qubit transmission



# Conclusions

# Take-away messages



- Quantum communication facilitates secure exchange of quantum information
- It requires an underlying optical fiber or free space infrastructure
- It needs classical communication for management & control
- It is an area of early research and requires a multi-disciplinary approach
- Quantum key distribution is the practical, near term application
- Complementing cryptography, it enables quantum-safe encrypted communication
- It is a stepping stone towards the vision of a future Quantum Internet



# Thank you

info@adva.com

#### IMPORTANT NOTICE

ADVA is the exclusive owner or licensee of the content, material, and information in this presentation. Any reproduction, publication or reprint, in whole or in part, is strictly prohibited. The information in this presentation may not be accurate, complete or up to date, and is provided without warranties or representations of any kind, either express or implied. ADVA shall not be responsible for and disclaims any liability for any loss or damages, including without limitation, direct, indirect, incidental, consequential and special damages, alleged to have been caused by or in connection with using and/or relying on the information contained in this presentation. Copyright © for the entire content of this presentation: ADVA.