Q bird

quantum connectivity

Dr. Ingrid Romijn

Co-Founder & CEO

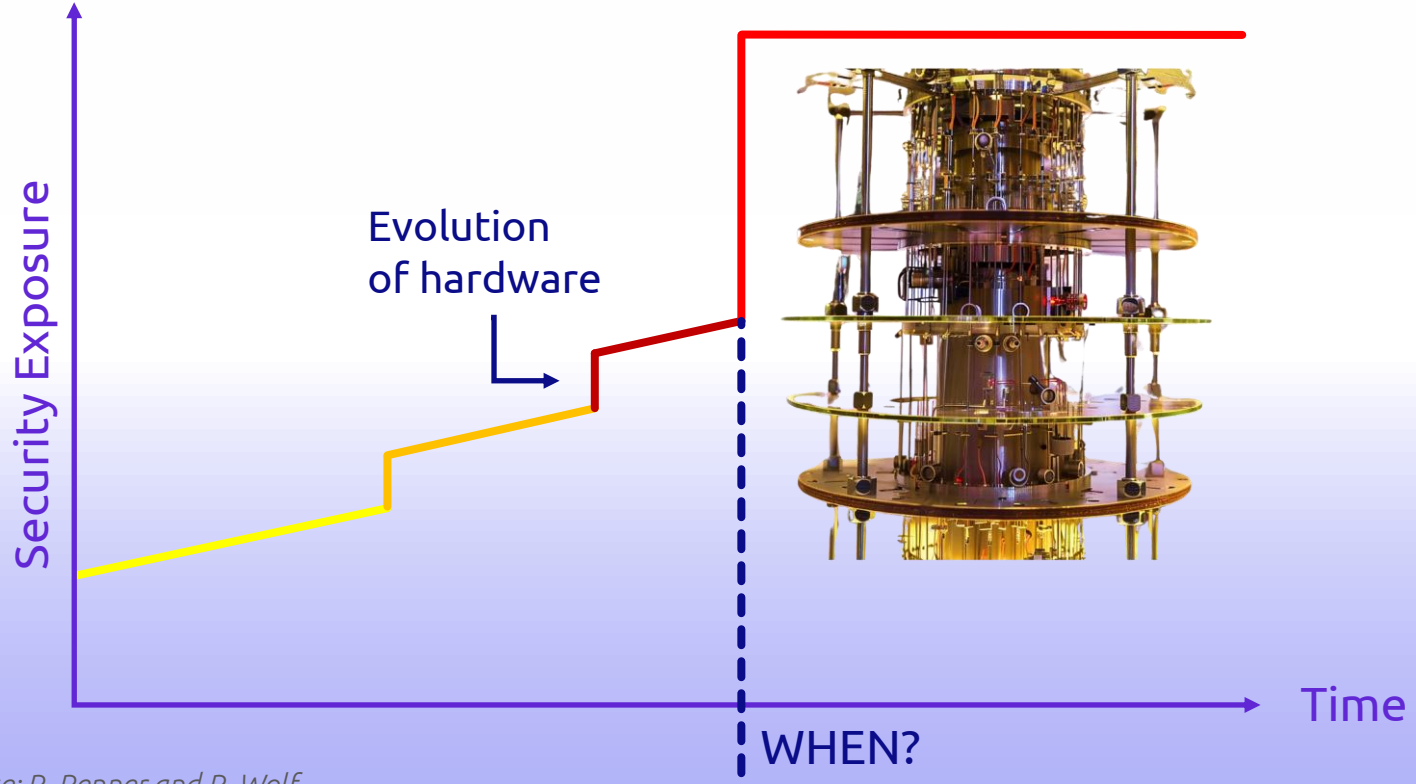
We are Q*Bird

- Delft-based leader in **Quantum Secure Communications**
- **We build ultra-secure networks** for critical infrastructure, government, finance and telecom
- Q*Bird **safeguards critical data** today and prepare for the **quantum internet** of tomorrow

Our Mission

- **Make Quantum Connectivity a reality**
- By securing communications using **Measurement Device Independent Quantum Key Distribution**
- By pioneering global **quantum connectivity** solutions that will link quantum processors, sensors and modems

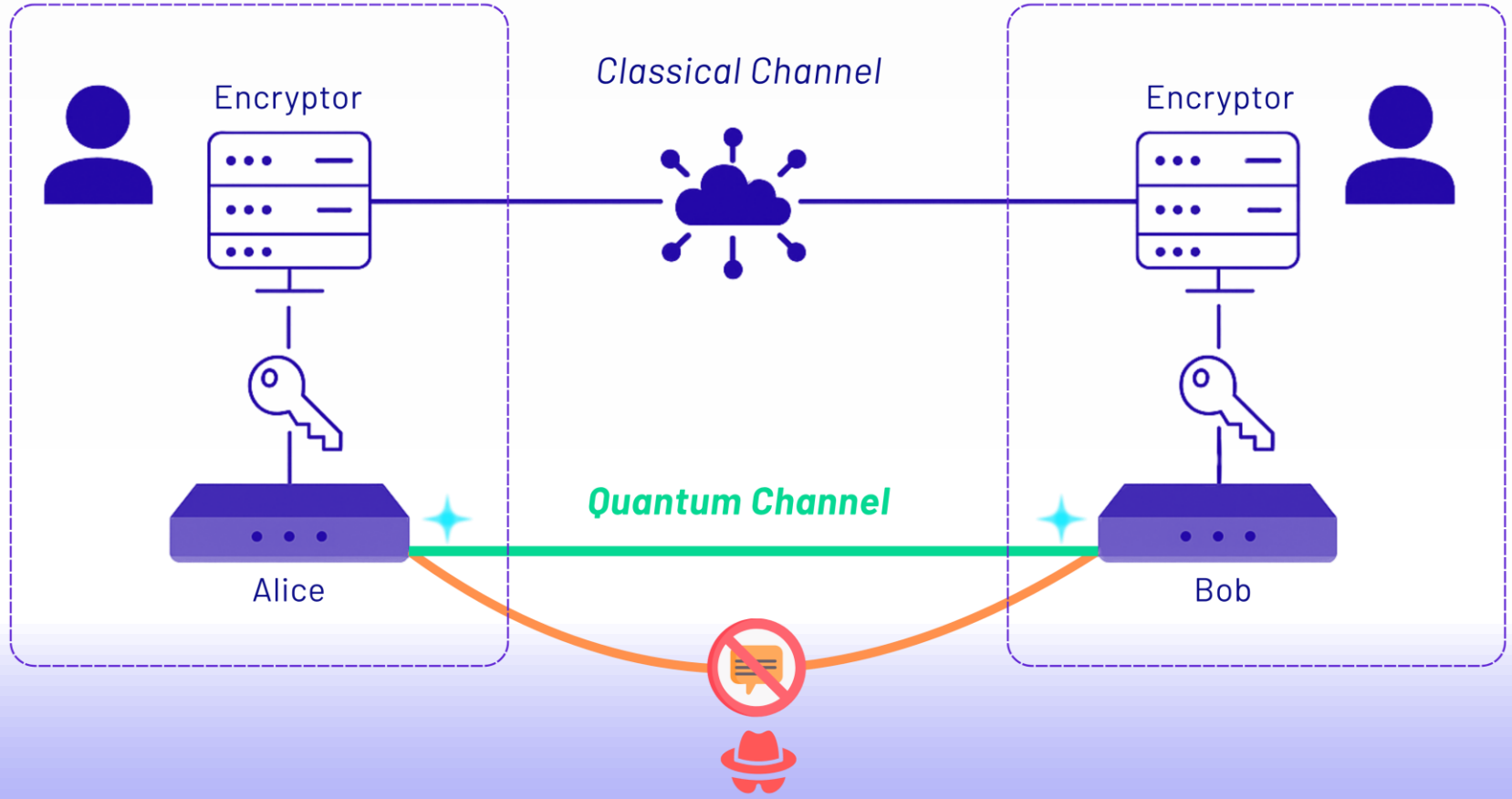
Why Quantum Security Matters?



- Traditional cryptography is increasingly vulnerable
- Quantum computers will break current cryptography
- *"Harvest now, decrypt later"* is already real and growing threat

Source: R. Renner and R. Wolf. "Quantum advantage in cryptography." AIAA Journal 61.5 (2023): 1895-1910

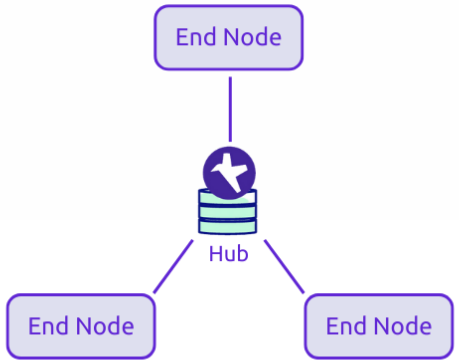
First-Generation Quantum Networks



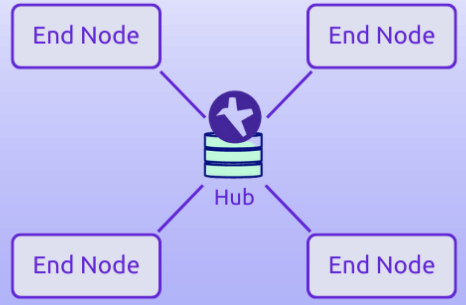
Our Solution

Secure Quantum Connectivity with Falqon® Series

3 User End Nodes



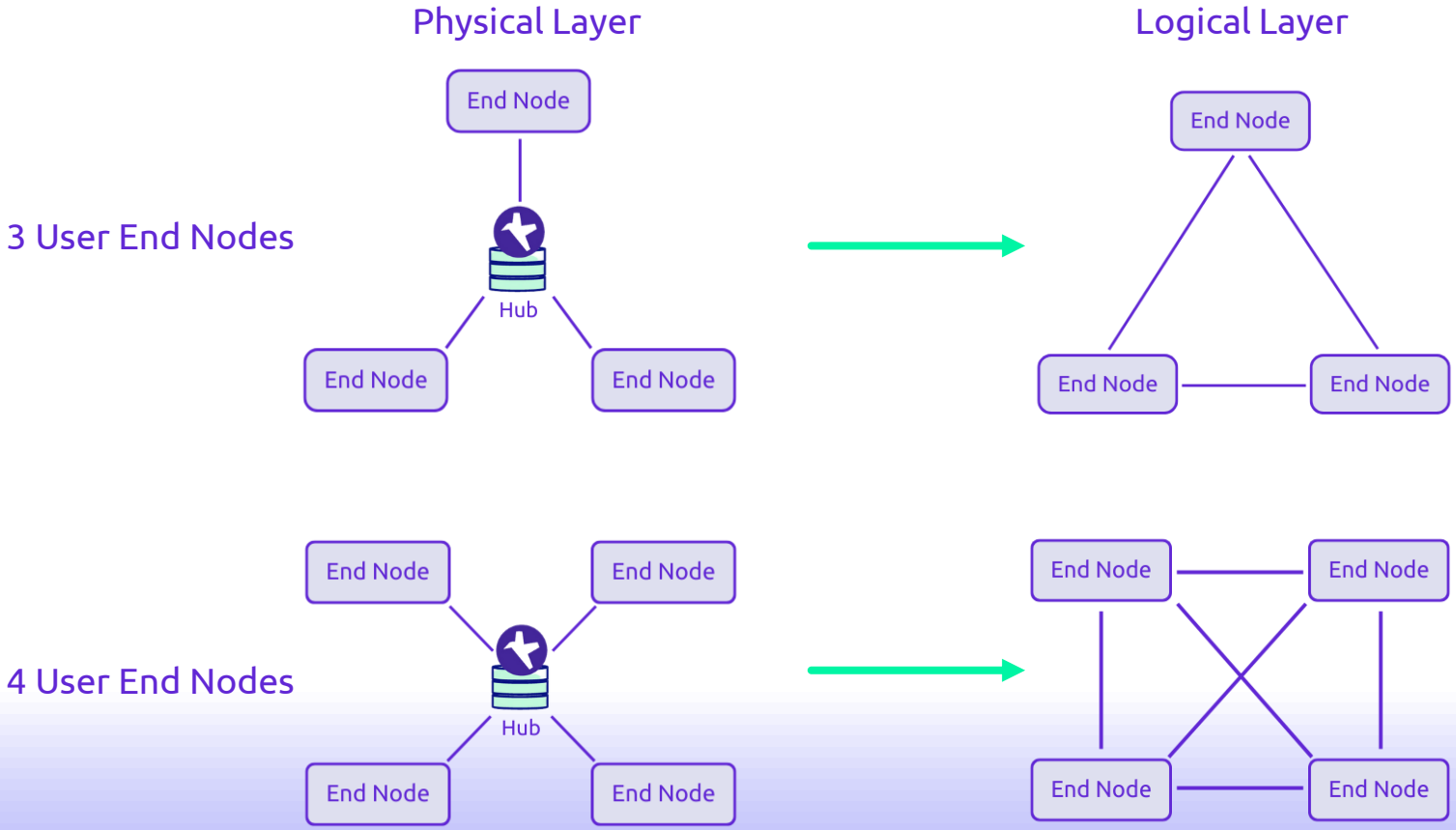
4 User End Nodes



- **Scalable Multi-User Connectivity with MDI-QKD**
- **Enhanced Security by Design**
- **Cost Effective for Network Scaling**
- **Built-In Redundancy**
- **Future-Ready Upgradability**

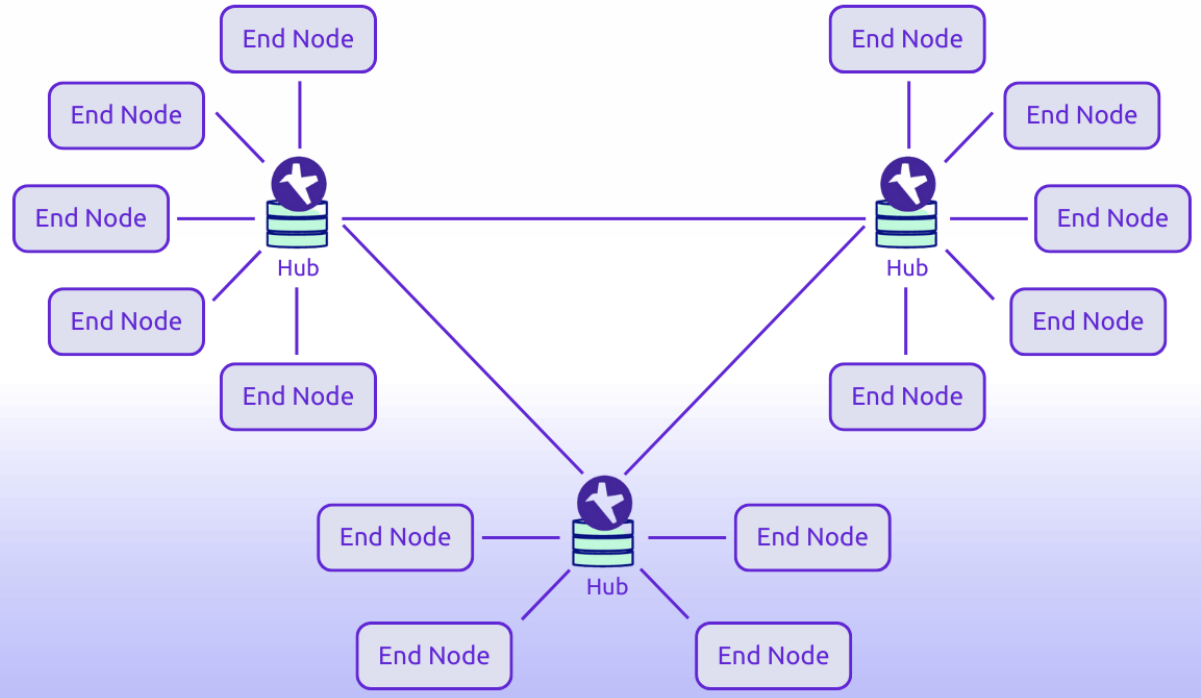
Our Solution

Secure Quantum Connectivity with Falqon® Series



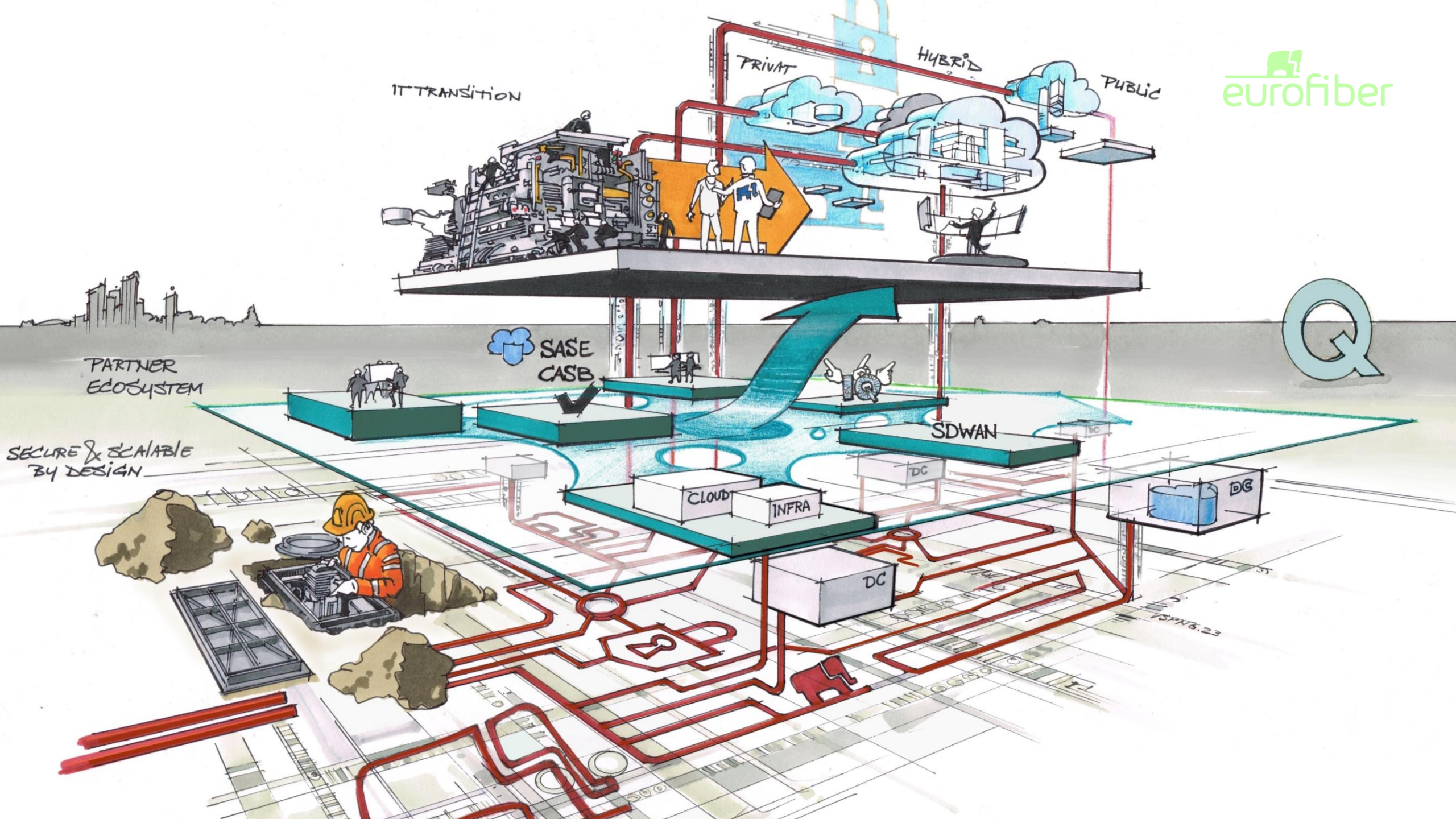
Our Solution

Network Friendly and Ready for Growth



- Extending Secure Connections up to 200 Km - 40 dB
- Multi-Point Quantum Connectivity
- Multi-Tenancy Architecture
- Scalable Connectivity

QKD network with **3 Center Hubs** and **14 End Nodes = n*(n-1)/2 = 91 connection pairs without trusted nodes!**


IT TRANSITION
PRIVAT
HYBRID
PUBLIC
PARTNER ECOSYSTEM
SECURE & SCALABLE BY DESIGN
SASE
CASB
SDWAN
CLOUD
INFRA
DC
DC
DC
DC
eurofiber

Business development

Strategic partnerships

Emerging technology

Marc Hulzebos
Business Innovation Officer
Eurofiber Group

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Alle publicaties >

Maak je organisatie quantumveilig

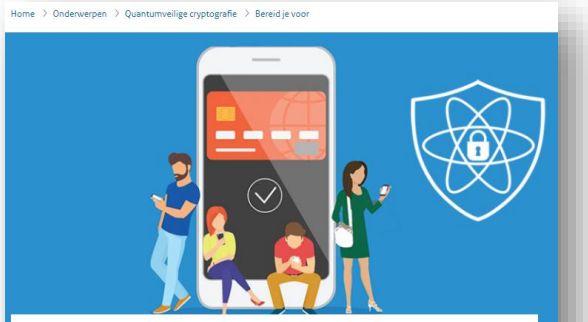
De ontwikkeling van een krachtige quantumcomputer is de laatste jaren in een stroomversnelling geraakt. Organisaties moeten nu in actie komen en zich gaan voorbereiden om tijdig te kunnen migreren naar quantumveilige cryptografie. De verwachting van experts is dat quantumcomputers tussen 2030 en 2040 waarschijnlijk over voldoende rekenkracht zullen beschikken om veel van de meest gebruikte vormen van cryptografie te kunnen breken.

Download in Nederlands: 'Maak je organisatie quantumveilig'

PDF document | 13 pagina's | 772 kB
Publicatie | 18-09-2023

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en het Nationaal Cyber Security Centrum (NCSC) hebben daarom een gezamenlijke handreiking 'Maak je organisatie quantumveilig' gepubliceerd. Deze handreiking is een aanvulling op het recent gepubliceerde PQC-migratiehandboek en biedt een nadere uitwerking van de daarin beschreven stappen en maatregelen.

Home > Onderwerpen > Quantumveilige cryptografie > Bereid je voor



Bereid je voor

Veel (overheids)organisatie en IT-leveranciers moeten zich nu al voorbereiden vanwege het risico dat quantumcomputers met zich meebrengen. Bijvoorbeeld organisaties die data verwerken, die over langere tijd nog vertrouwelijk moeten blijven, of die systemen met een lange levensduur aanbieden.

Het PQC-migratie handboek van de AIVD geeft criteria voor wanneer je nu al moet beginnen. Je bent dan een zogenaamde 'urgente adopter'. Dat ben je als te maken hebt met:

- Gevoelige informatie van de organisatie met een lange vertrouwelijkheidstermijn ('store now decrypt later');
- Persoonlijke informatie met een lange vertrouwelijkheidstermijn: paspoorten;
- Aanbieden van systemen voor de kritieke infrastructuur: betalingsverkeer, energie, transport;

Dutch IT Leaders

Thema's | Evenementen | Agenda | Dutch

HR | Talent | Diversity | Future of Business Technology | Culture & Leadership | Sustainability | Gre

WITOLD KEPINSKI - 21 SEPTEMBER 2023 Deel dit artikel

NCSC: maak je organisatie quantum veilig

De ontwikkeling van een krachtige quantumcomputer is de laatste jaren in een stroomversnelling geraakt. Organisaties moeten nu in actie komen en zich gaan voorbereiden om tijdig te kunnen migreren naar quantumveilige cryptografie. De verwachting van experts is dat quantumcomputers tussen 2030 en 2040 waarschijnlijk over voldoende rekenkracht zullen beschikken om veel van de meest gebruikte vormen van cryptografie te kunnen breken.

Quantum computing | Quantum technologie | Security | Cybersecurity

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en het Nationaal Cyber Security Centrum (NCSC) hebben daarom een gezamenlijke handreiking 'Maak je organisatie quantumveilig' gepubliceerd. Deze handreiking is een aanvulling op het recent gepubliceerde PQC-migratiehandboeken biedt een nadere uitwerking van de daarin beschreven stappen en maatregelen.

Aan de slag met het voorbereiden op de migratie naar

DUTCH IT EVENTS

GLOBAL RISK INSTITUTE

Read | Attend | Watch | About | Resources | News

6 DECEMBER 2024

Cyber Risks | Operational Resilience | Technology Innovations

Quantum Threat Timeline Report 2024

Global Risk Institute

Download Full Report PDF | Download Executive Summary PDF

Intelligence agencies don't like encryption with Quantum Key Distribution

Recent in Security

- Fortinet warns vulnerability in FortiClientEMS is exploited in the wild
- Personal data exposed at Air Europa
- Dutch researcher discovers Fujitsu blunder: AWS keys and logins in public bucket
- Windows and Exchange Servers crash after March 2024 update
- Care retailer of Belgian health insurance provider victim of data breach

Jobs - Techcareer

IT en Telecom Engineer
Duiven | Full time

Senior Data Engineer – Marketing Automation (AWS)
Den Haag | Full time

Several European intelligence agencies voiced their criticism about Quantum Key Distribution (QKD) in a recent position paper. This encryption method

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Alle publicaties

Maak je organisatie quantumveilig

Home > Onderwerpen > Quantumveilige cryptografie > Bereid je voor

Dutch IT Leaders

Thema's Evenementen Agenda Dutch

HR | Talent | Diversity Future of Business Technology Culture & Leadership Sustainability | Gre

WITOLD KEPINSKI - 21 SEPTEMBER 2023 Deel dit artikel

NCSC: maak je organisatie quantum veilig

WIRED

SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH

SIGN IN SUBSCRIBE

THE BIG STORY

The Quantum Apocalypse Is Coming. Be Very Afraid

What happens when quantum computers can finally crack encryption and break into the world's best-kept secrets? It's called Q-Day—the worst holiday maybe ever.

AMIT KATWALA

MAR 24, 2025 6:00 AM

Global Risk Institute

Download Full Report PDF

Download Executive Summary PDF

provider victim of data breach

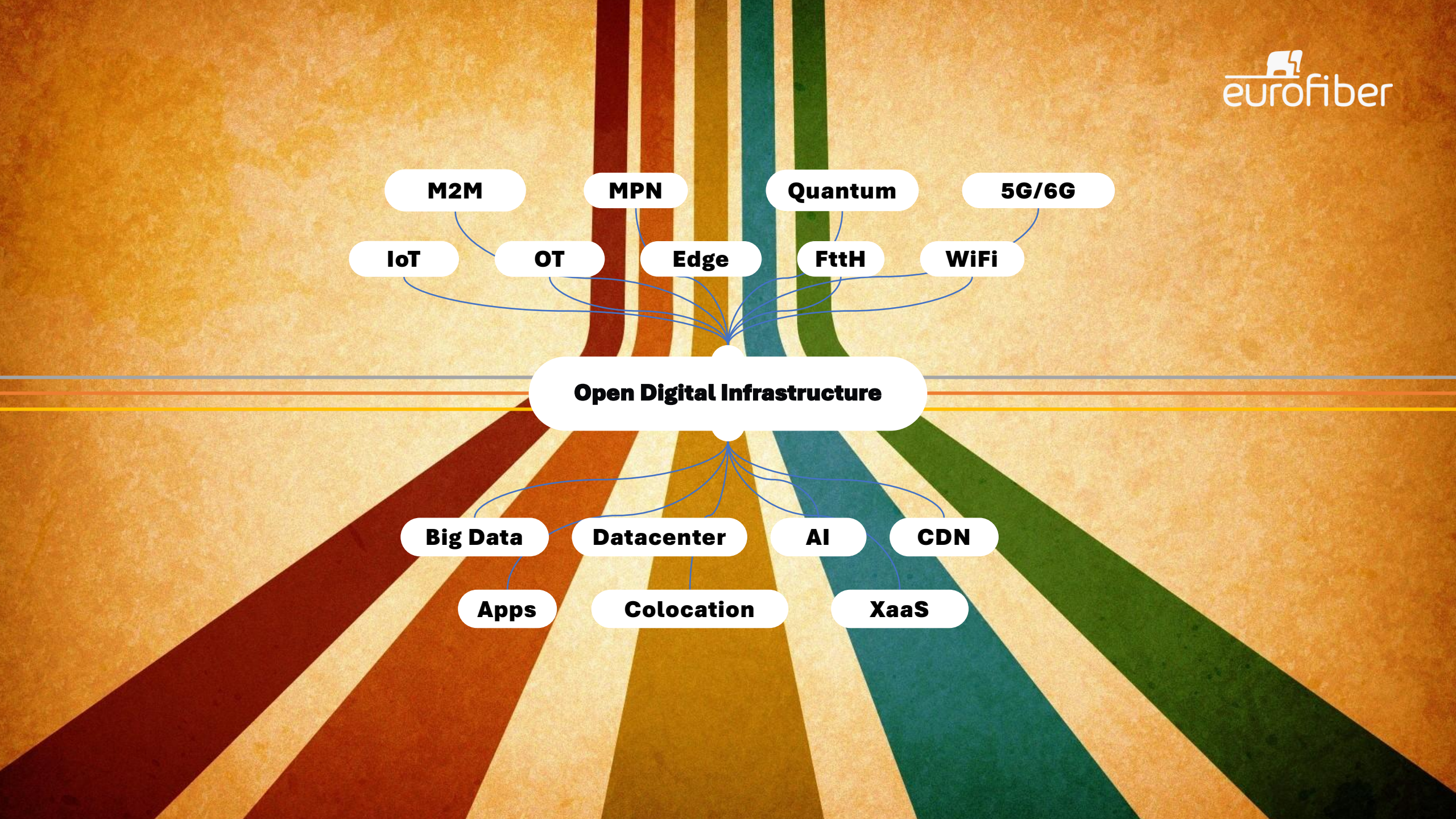
Jobs - Techcareer

IT en Telecom Engineer

Senior Data Engineer – Marketing Automation (AWS)

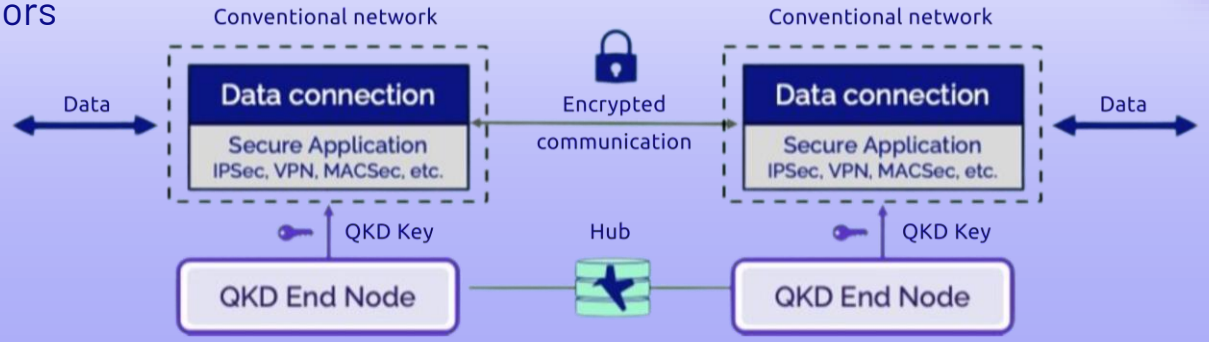
Several European intelligence agencies voiced their criticism about Quantum Key Distribution (QKD) in a recent position paper. This encryption method

eurofiber


eurofiber
M2M
MPN
Quantum
5G/6G
IoT
OT
Edge
FttH
WiFi
Open Digital Infrastructure
Big Data
Datacenter
AI
CDN
Apps
Colocation
XaaS

What Makes Falqon® Ready for Scalable and Secure Network Architectures?

- **Data Center compatible**: 19-inch rack mountable
- **Devices**: Center Hub, Quantum Switch, End Nodes
- **Architectures**: n-to-n star networks, rings, other complex network architectures capable
- **Integrated key management system**
- **Multiplexing**: possible (O-band, C-band)
- **Interfaces**: with encryptors and cryptography applications; tested with major vendors



Powering Security: Q*Bird's Deployment Footprint

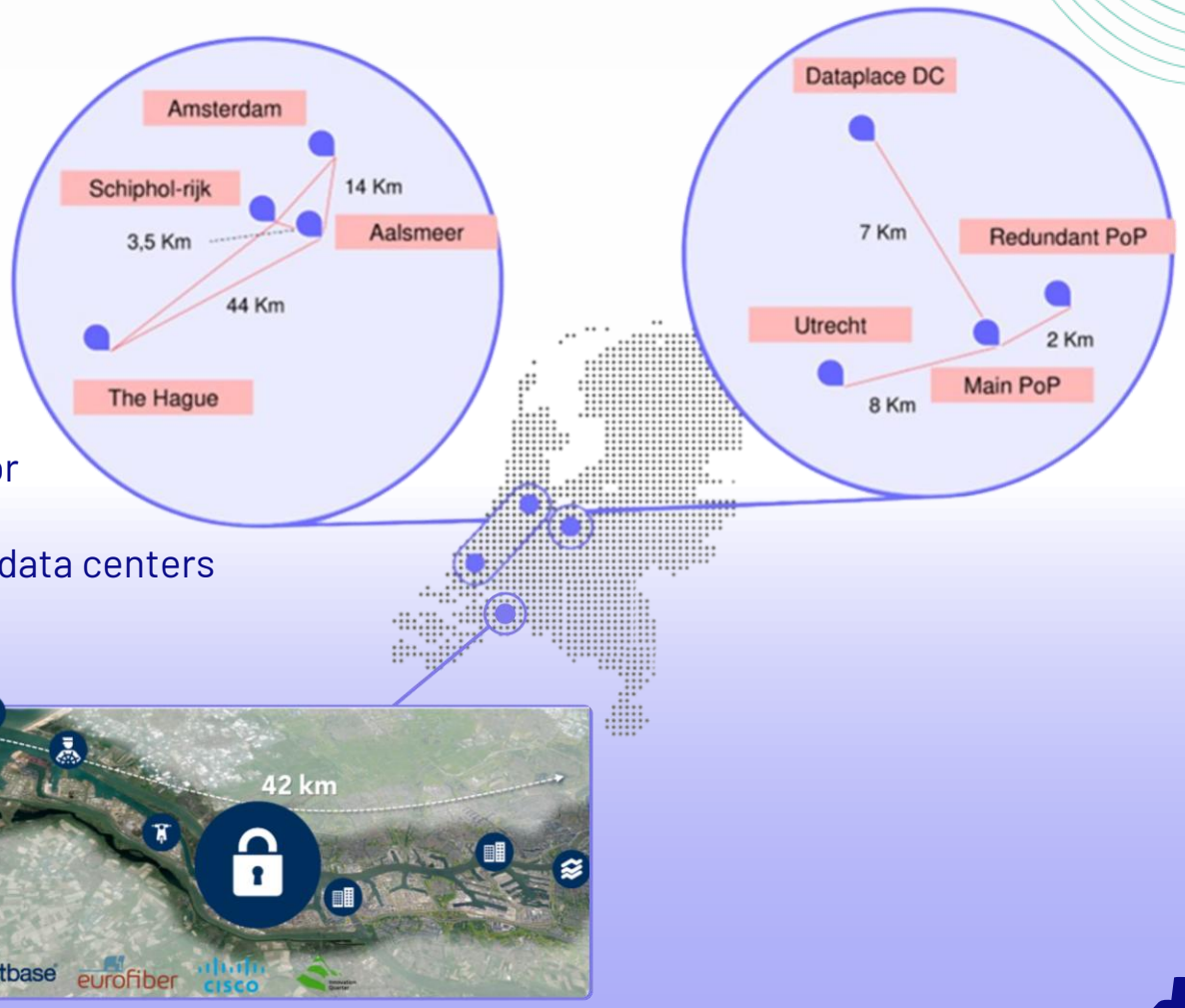
- **Integration** with Juniper & Cisco Line Encryption
- POC with **Dutch Bank**
- System installation in the **Port of Rotterdam**
- System installation in **Educational and Industrial Data Centers**
- System installation in **Dutch Government Data Centers**
- First **Cross-Border MDI QKD Quantum Network** deployment in Benelux together with Belnet as part of BeQCI Consortium

Scalable Quantum Networks in Multiple Locations

Connect to conventional networks

Test Use Cases:

- **In the Port of Rotterdam:** Securing Europe's largest harbor
- **Amsterdam to The Hague:** Securing Dutch governmental data centers
- **Utrecht area:** Securing educational network



Use Case – Port of Rotterdam

- **High Frequency** e.f. Water levels, ship positions
- **High Confidential** e.f. Container inspections
- **Multi-User** e.f. Port calls

Why Would the Port of Rotterdam Get Involved?

DP World Australia has been the target of a cyber attack (source: DP World)

Cyber attack takes out DP World Australia port operations

13 Nov 2023 by Jamey Bergman

Suez Canal: What Was the Blockage's Impact on the Global Economy?

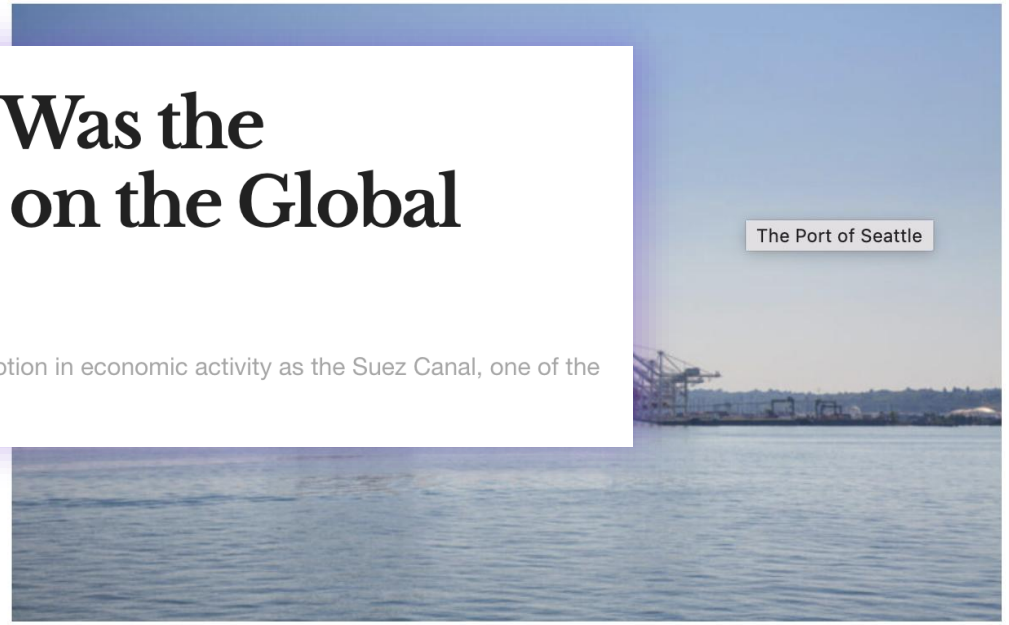
> In late March 2021, the world witnessed a major disruption in economic activity as the Suez Canal, one of the most important waterways in the world, was blocked.

Port of Seattle shares details of a cyberattack

September 19, 2024

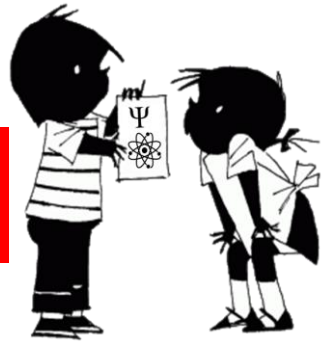
By Syed Rakin Rahman

TWITTER FACEBOOK LINKEDIN EMAIL



The Port of Seattle has isolated its critical systems after the port identified system outages consistent with a cyberattack last month.

Quantum security trial Port of Rotterdam



Location A

Location B

DATACENTER

CENTERNODE

ENDNODE

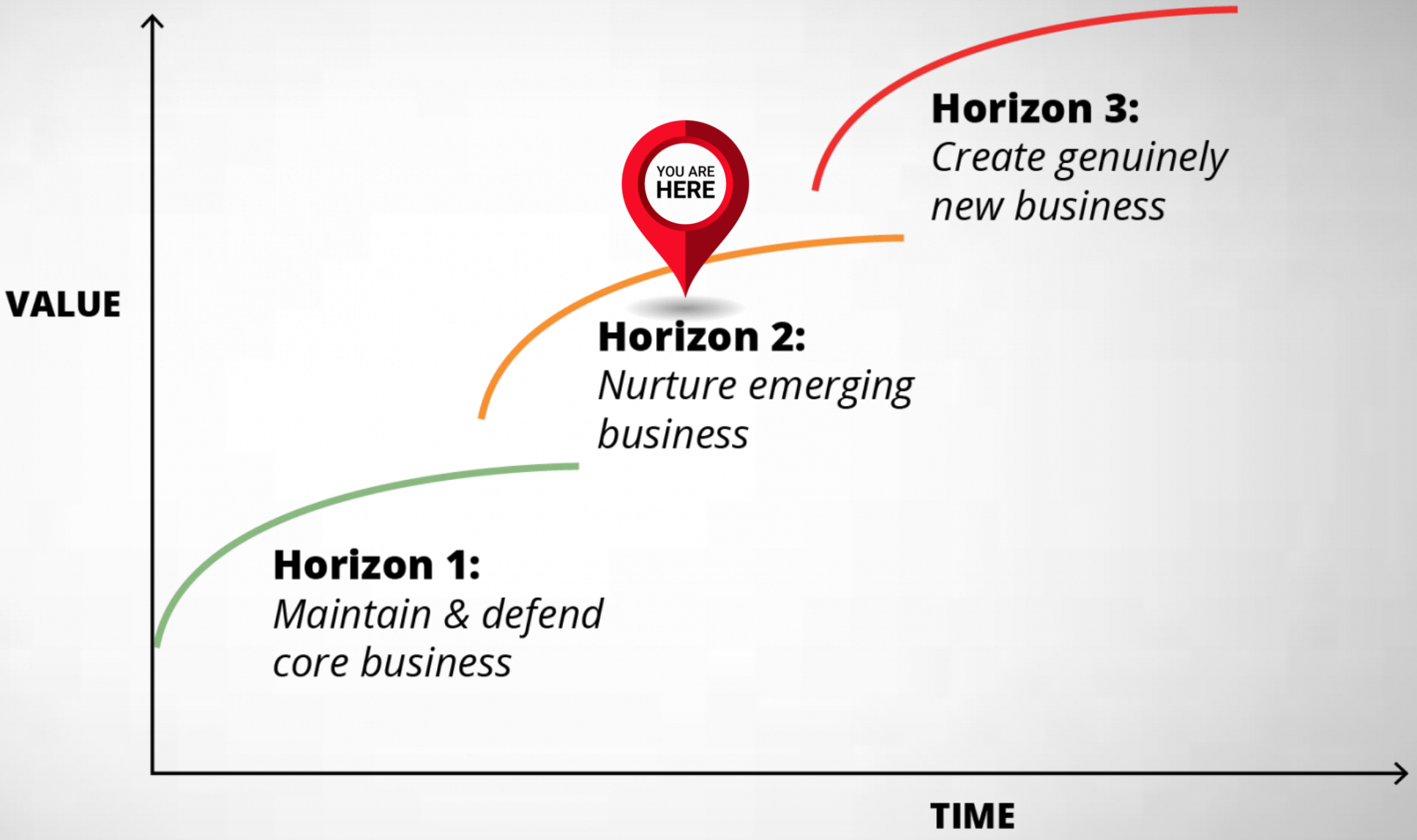
ALICE

CHARLIE

ENDNODE

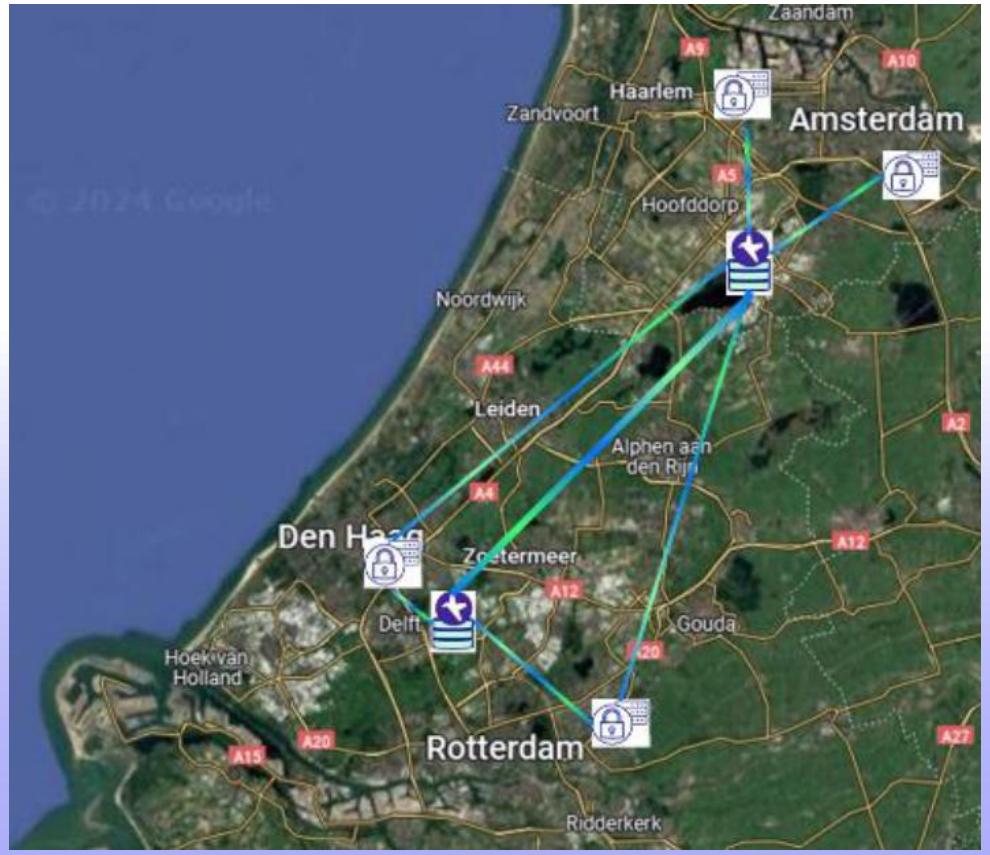
BOB


Business
Strategy and vision
Market demand
Compliance
Operations
Products
Technology
Digital tools & platforms
Automation efficiency
Data analytics
Cloud computing
Cybersecurity
Digital transformation
QUEST
New businessmodels
Emerging technology
Innovation
Strategic partnerships
New products/ services
Disruption & transformation
Experimentation
Adaptability

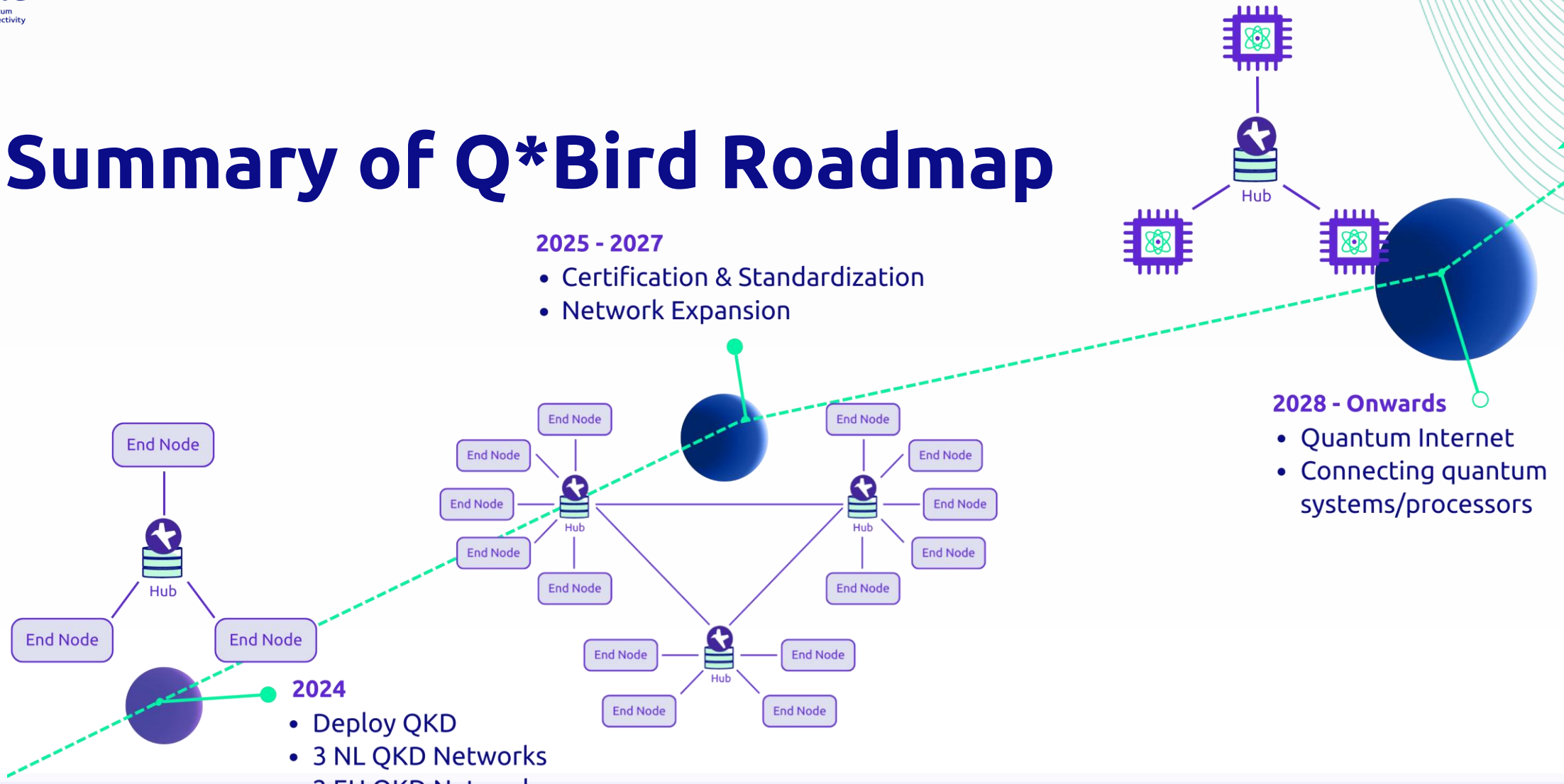

VALUE
TIME
YOU ARE HERE
Horizon 1:
Maintain & defend core business
Horizon 2:
Nurture emerging business
Horizon 3:
Create genuinely new business

QUEST: Expanding the network

- **Dual homing End Nodes** & build in redundancy
- **Additional Center Hub** in the network
- **New users are welcome to join and secure their data by**
  - connecting their own End Node
  - Using QKD as a Service through Eurofiber data centers



Summary of Q*Bird Roadmap



- Lay the foundations for quantum internet.
- Deploy quantum-secured networks for data centers, critical infrastructures, governments, EuroQCI.

- Towards general purpose quantum internet.

Q bird

quantum
connectivity

Secure Quantum Connectivity

www.q-bird.com ingrid@q-bird.com q-bird ItsQBird