Quantensichere Kommunikation in Europa

Roland Abfalterer, NTS Senior Security Architect
Lukas Helm, zerothird, Head of Sales

Wie sicher ist unsere Kommunikationstechnologie?

Bedrohungen

- Quanten Computer (QC)

Schwachstellen

- Klassische Kryptographie PKIs, TLS können mittels **Shor**-Algorithmus effizient gebrochen werden (Signaturen, Schlüsselaustausch etc.)

Risiken

- Datenströme können jetzt gespeichert, später durch QC entschlüsselt werden (VPNs, https,) – längerfristig
- Daten Leaks: CA's gefälscht, Private Keys errechnet

Wir Sicherheitsverantwortlichen müssen uns jetzt vorbereiten.

ZERO/3

NTS

Wie können wir uns schützen?

BSI, NIST: empfehlen Post Quantum Cryptography (PQC)

- Sicherheit beruht auf mathematischer Komplexität
- Relativ jung, noch nicht umfangreich erforscht

Quantum Key Distribution (QKD)

- Sicherheit beruht auf Natur-Gesetzen der Quantenmechanik
- Gesetze mehr als 100 Jahre intensiv experimentell geprüft
- Noch nicht großflächig einsetzbar in Europa

Wir schauen uns heute QKD näher an – was fehlt noch in Europa?

ZERO/3

NTS

100 Jahre Quantenforschung

1925: Geburt der Quantenmechanik

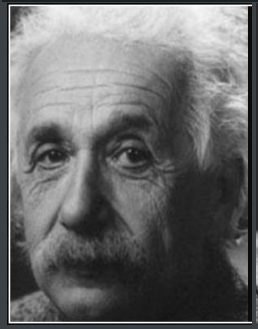
1935: Quantenverschränkung (Schrödingers Katze)

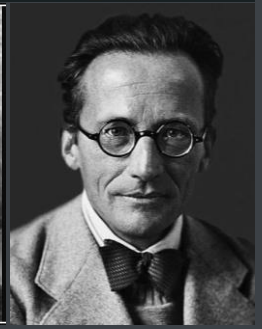
1970er: Quanteninformatik

1984: Protokoll zur Quantenkommunikation

1994: Shor-Algorithmus

2001: Der erste Quantencomputer





ZERO/3

NTS

Stand 2025

Quantum Computing

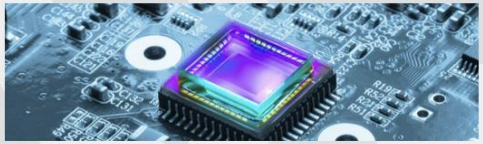
... uses quantum bits to perform calculations that are exponentially faster than classical computing. This includes machine learning, drug discovery, financial modelling and hacking of cryptographic systems using e.g. Shor's algorithm.

Quantum Communication

... uses the principles of quantum mechanics to transmit information in a secure and crack-proof way. Major application is Quantum Key Distribution ("QKD")/cryptography.

Quantum Key Distribution ("QKD")

Quantum Sensing



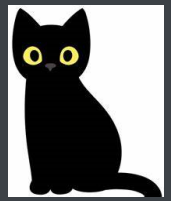
... aims to measure physical quantities with higher precision and to surpass classical sensors' limits. Applications include imaging, navigation, and environmental monitoring.

ZERO/3

NTS

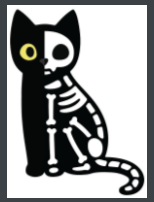
Bits und verschränkte Qubits

0



1

- beliebige Entfernung
- abhörsicher (Superposition)
- absolut zufällig



0,1

Verschränkung

0,1

ZERO/3

NTS

Quantensichere Kommunikation (QKD)

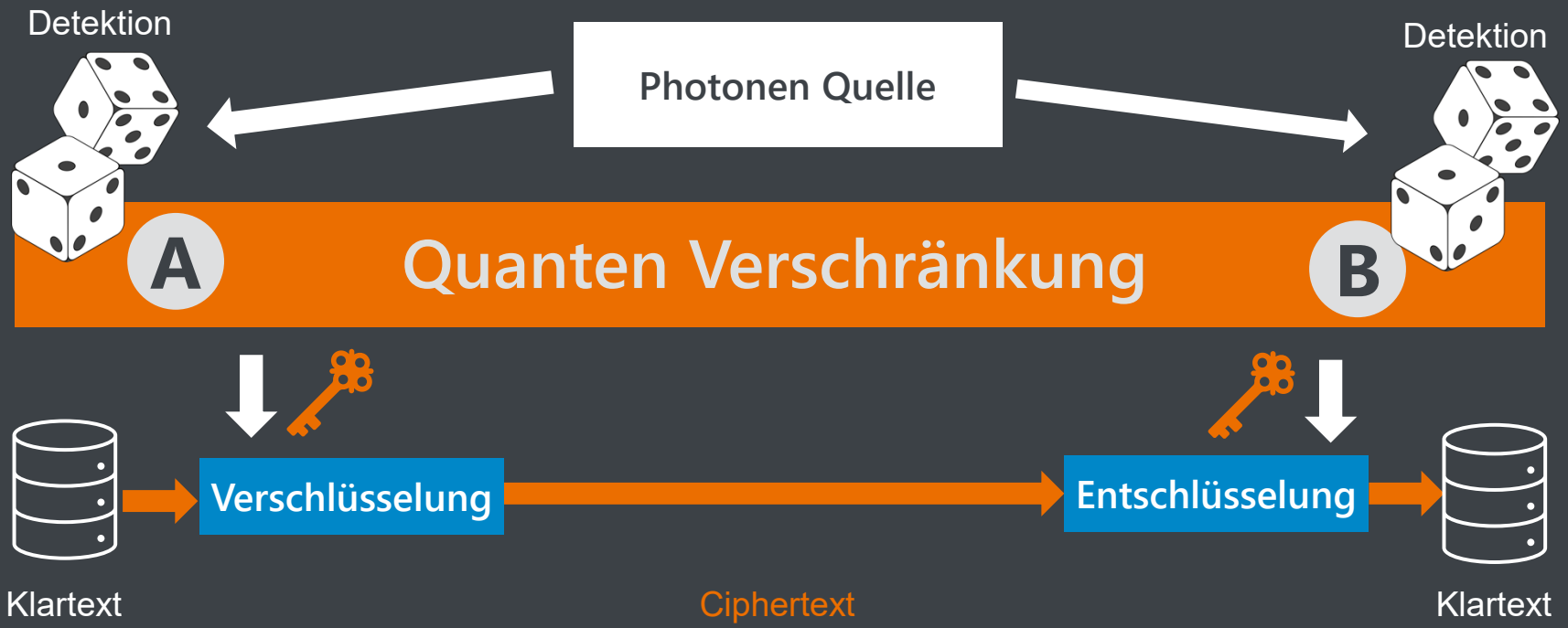
Schlüssel links: 0100100010000011111.....

Schlüssel rechts: 0100100010000011111.....

ZERO/3

NTS

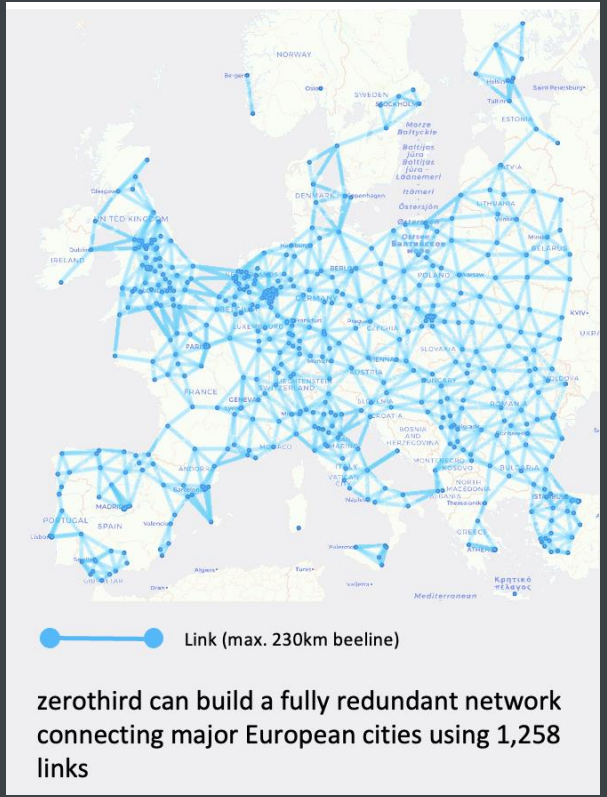
Quantensichere Kommunikation (QKD)



ZERO/3

NTS

Quantensicheres Europa

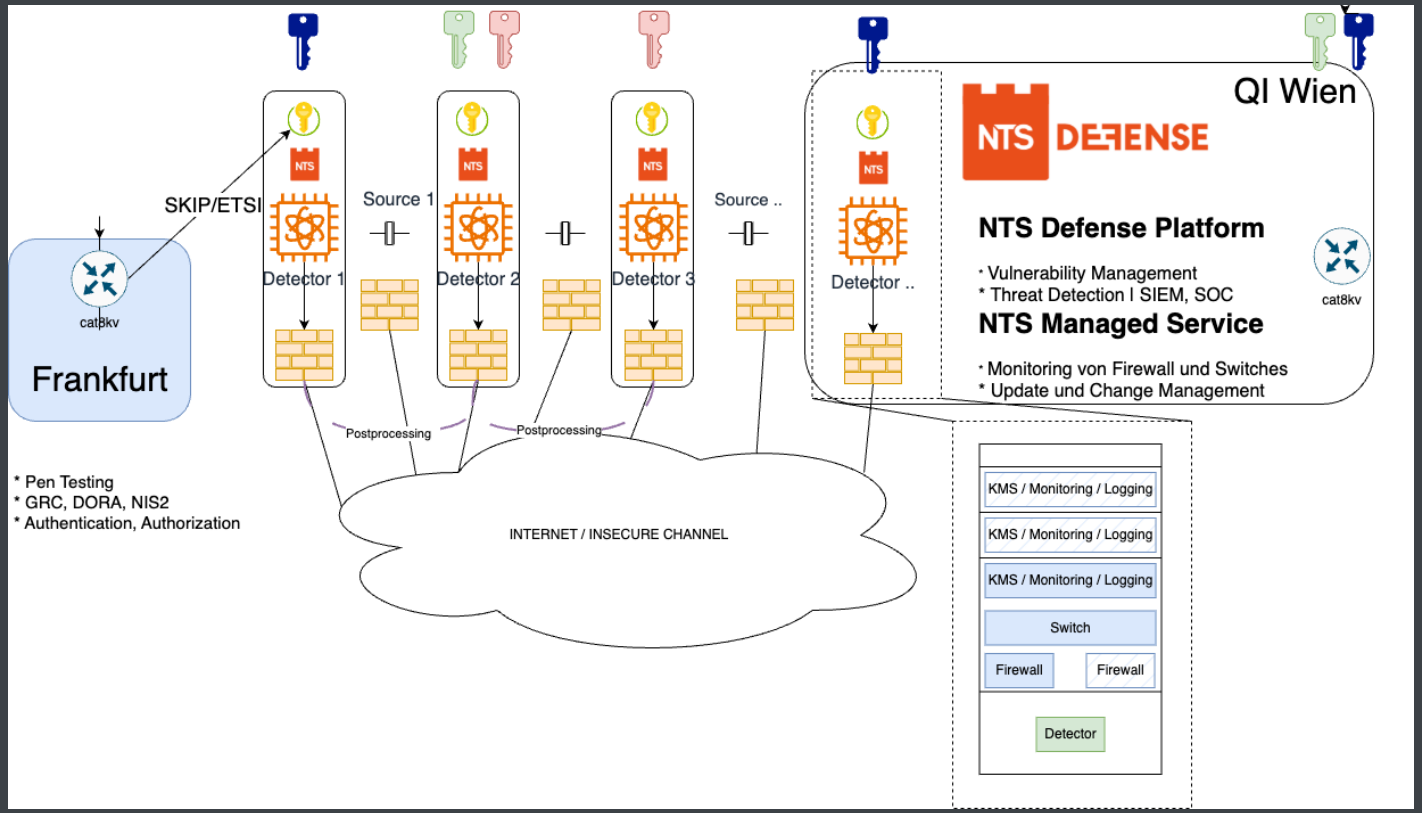


zerothird can build a fully redundant network connecting major European cities using 1,258 links

ZERO/3

NTS

LANG DISTANZ ENTWURF ~1000KM



ZERO/3

NTS

Zusammenfassung

Die Sicherheit unserer heutigen Kommunikation kann durch QC gebrochen werden

- Es ist Zeit sich über das Thema zu informieren: PQC, QKD
- Technologien studieren, Architektur Review

Abschätzen - Wie groß ist das Risiko?

- Datenklassifizierung
- Kryptographie Atlas

Strategie wählen, Plan erstellen

- Risiko akzeptieren
- *Risiko Milderung durch **gezielten** Einsatz von PQC **und** QKD*

ZERO/3

NTS

Vielen Dank!

FRAGEN?

ZERO/3

NTS