The Road towards the Quantum Internet

Juniper Networks

Driven by Experience™

What is Quantum Network?

A **quantum network** is a system that uses the principles of quantum mechanics to transmit information securely

BIT VS QUBITs

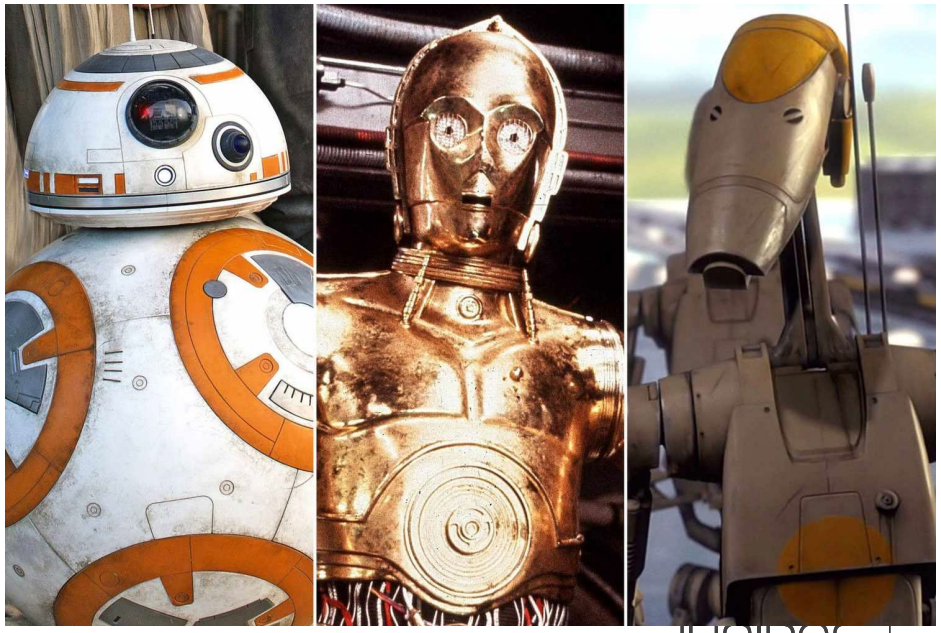
Our Quantum future

This innovation serves a purpose for humanity to utilise the computing power to drive innovation and advancement in tackling the following:

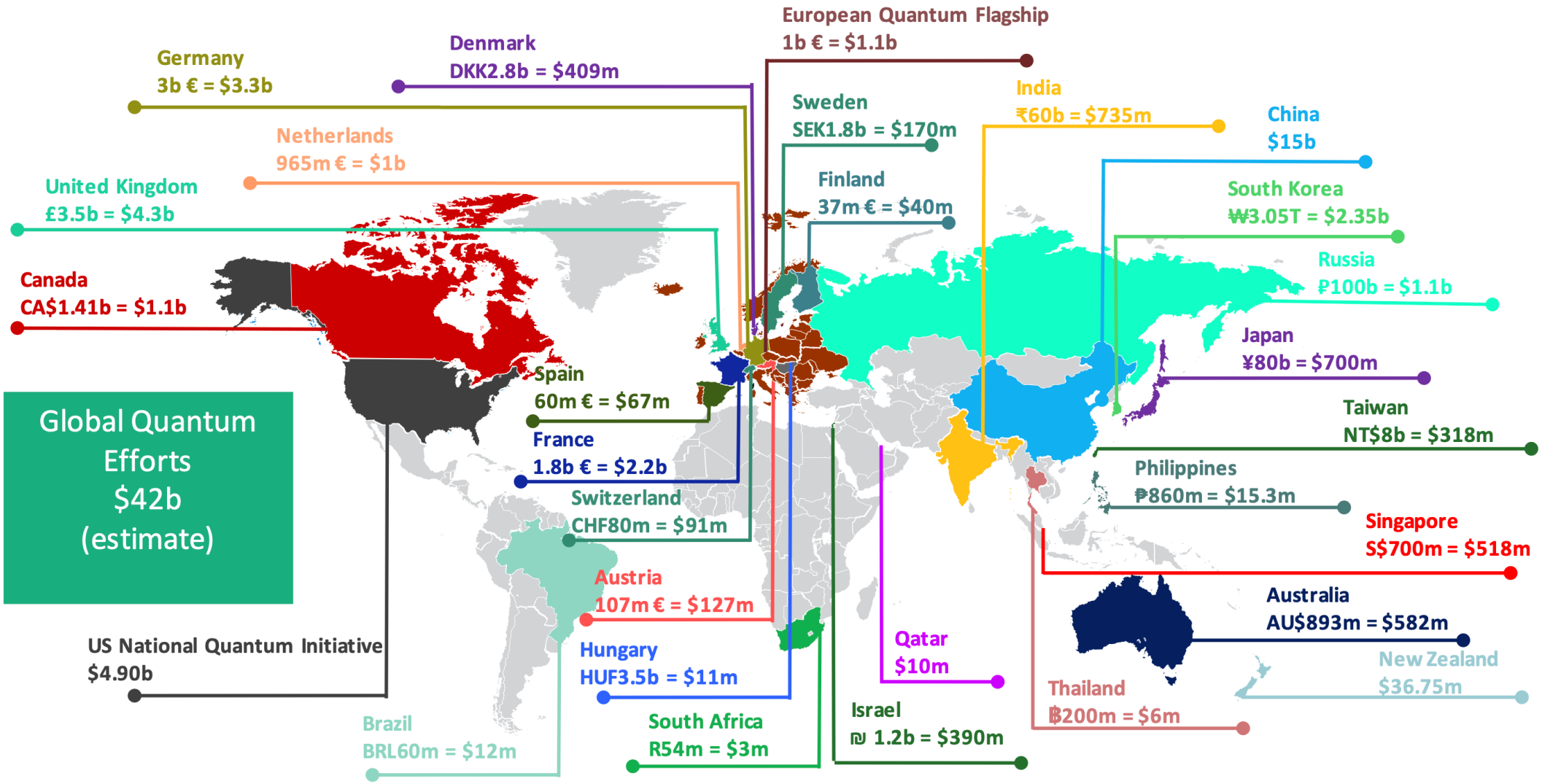
- Climate modelling
- Heath care new treatments for cancer
- Drug advancement
- Chemistry
- Agriculture and food technology
- New Communications technologies
- Even decode the human Genome

Why is this a threat

- Our current cryptographic algorithms, such as RSA and ECC, are based on mathematical problems that are hard to solve with classical computers.
- Quantum computers can exploit specific algorithms and factorize large numbers exponentially faster, compromising data security.
- The potential consequences are severe, affecting financial transactions, sensitive communications, and more.

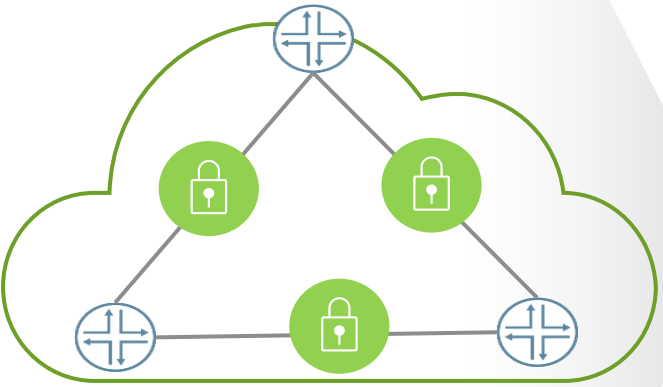


Quantum Technology Funding in 2023

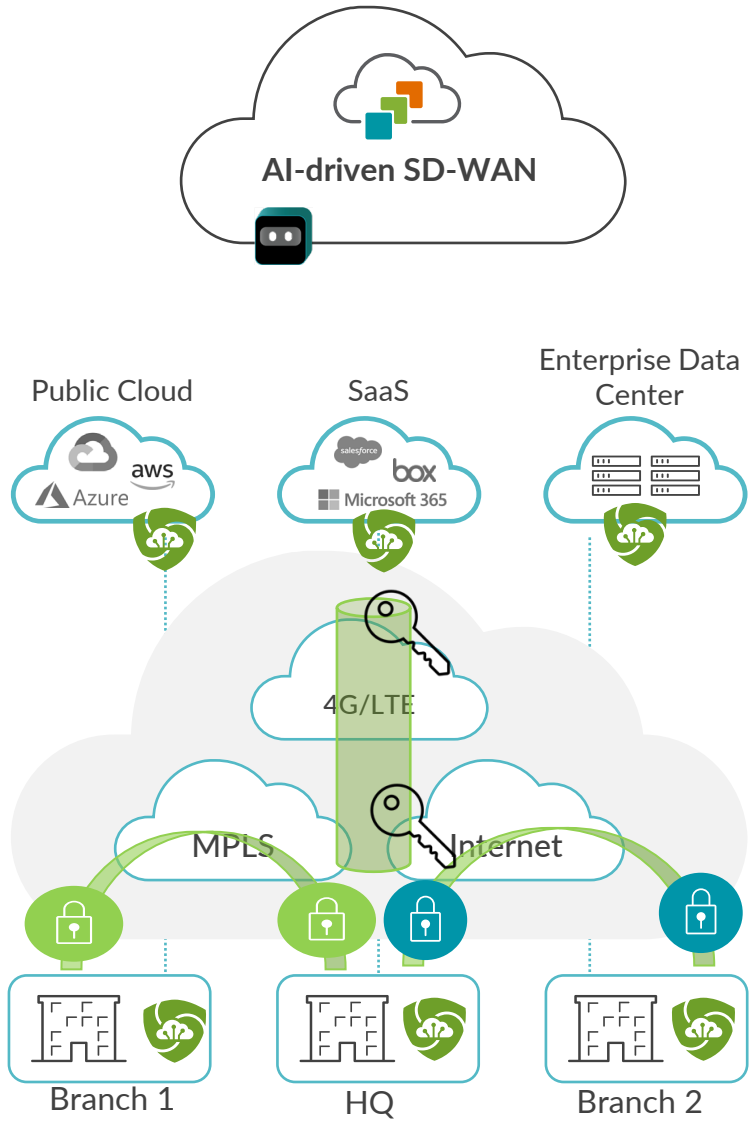


https://www.weforum.org/agenda/2023/01/the-world-quantum-divide-why-it-matters-davos2023

Quantum safe-networks



Quantum Secured
IP/MPLS Infrastructure



AI-driven WAN Assurance

Enhance Security

- Application Control
- Identity & Access Control
- Intrusion Prevention
- Antimalware
- Threat Intelligence
- Secure Web Access

IPsec Quantum Secured Tunnel

MACsec Quantum Secured Infrastructure

IPsec using Symmetric Key Distribution (DSKE)

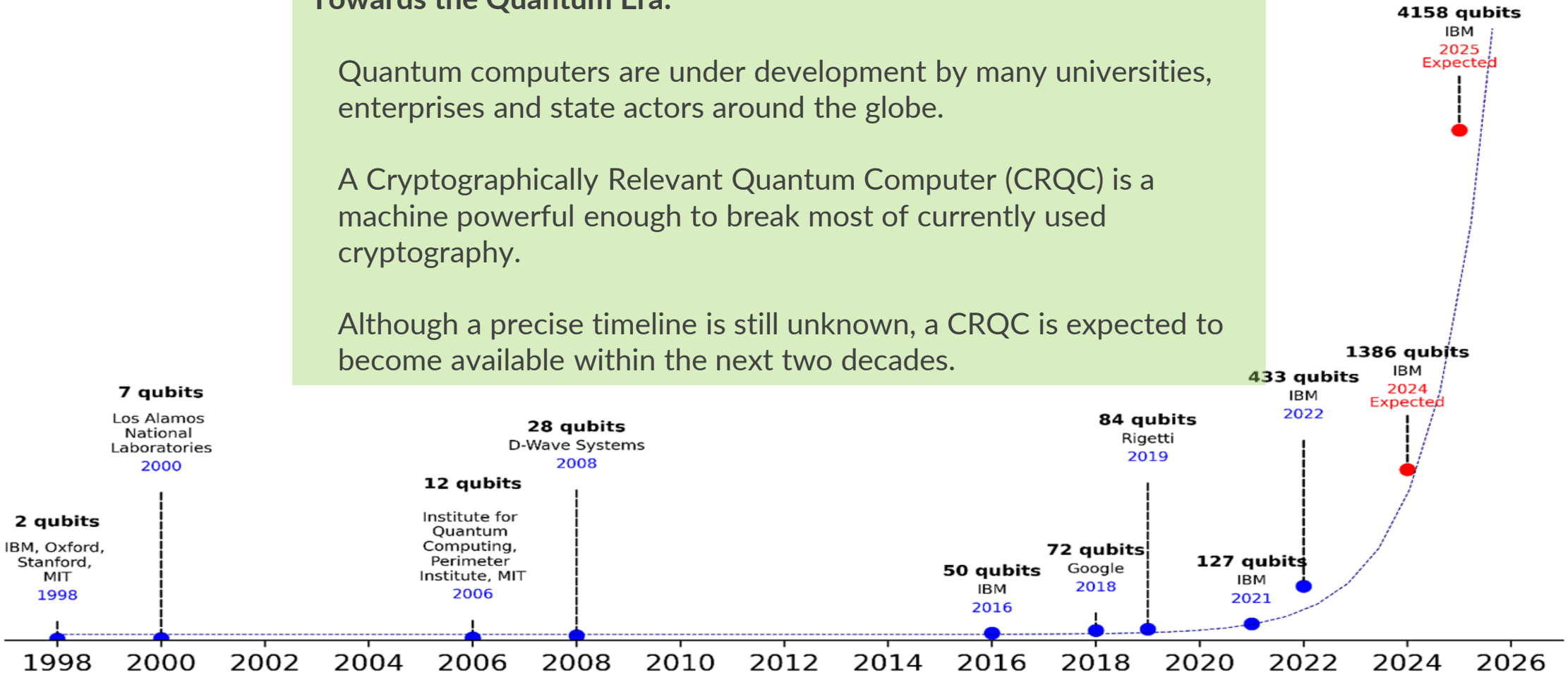
The Quantum Trend/Threat

Towards the Quantum Era:

Quantum computers are under development by many universities, enterprises and state actors around the globe.

A Cryptographically Relevant Quantum Computer (CRQC) is a machine powerful enough to break most of currently used cryptography.

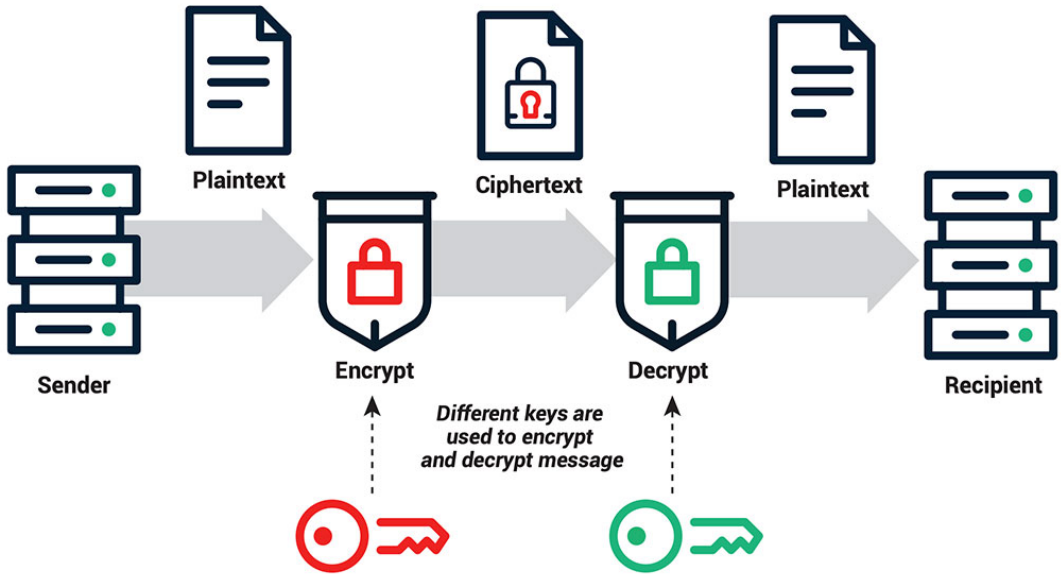
Although a precise timeline is still unknown, a CRQC is expected to become available within the next two decades.



https://www.nqsn.sg/

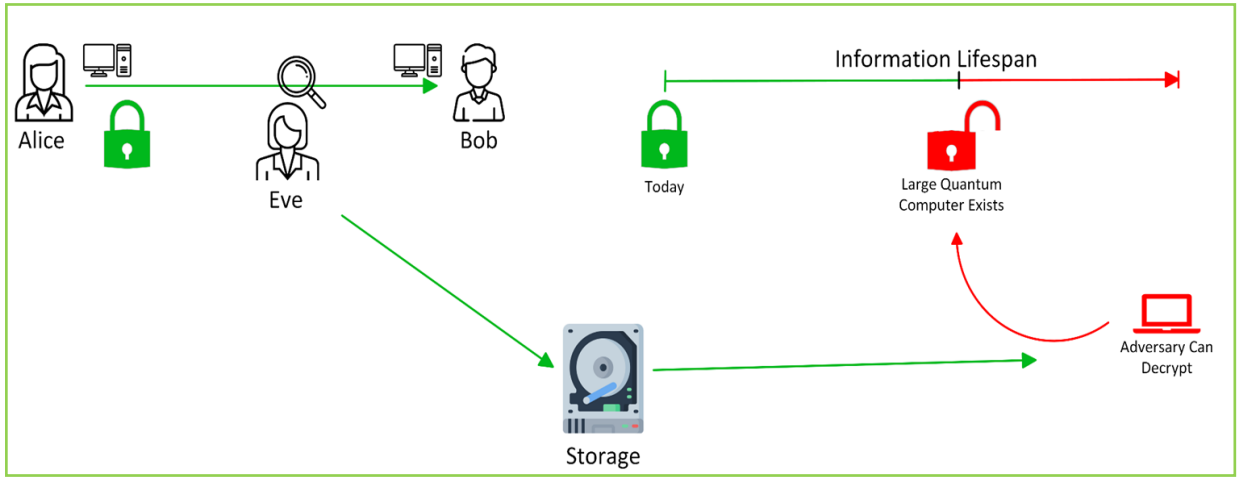
https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/sg-launches-southeast-asias-first-quantum-safe-network-infrastructure

Problem Statement – Asymmetric Cryptography



Problem 1:

Quantum Computing Capabilities: Quantum computers have the potential to solve complex mathematical problems much faster than classical computers. This includes breaking the cryptographic algorithms that currently secure our data. Traditional encryption methods, like RSA and ECC, rely on the difficulty of certain mathematical problems, which quantum computers can solve efficiently.



Problem 2:

- **Harvest now, decrypt later**: While powerful enough quantum computers are not available now, the concern/opportunity is in attackers stealing and storing encrypted data to decrypt with the quantum computers of tomorrow.

Conclusion:

- Asymmetric cryptography as it exists today is not, and cannot, therefore be 'quantum secure'.

The need for Quantum Safe-Networks

1. **Protecting Sensitive Data**:

As quantum computers advance, they will be able to break current encryption methods, putting sensitive data at risk. Quantum safe-networks use quantum technology (which has multiple options) to ensure that data remains secure even against quantum attacks.

2. **Regulatory Compliance:**

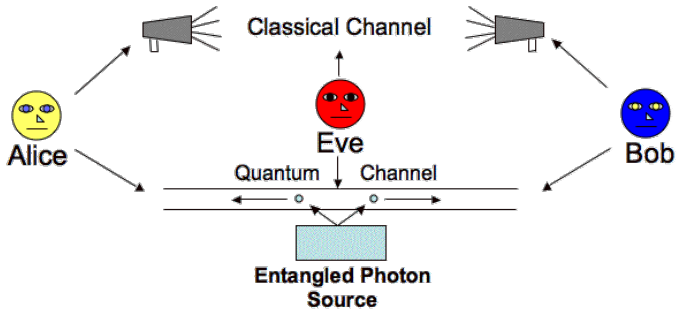
Many industries are subject to strict data protection regulations. Implementing quantum-safe technologies helps organizations comply with these regulations and avoid potential legal and financial penalties

3. **Future-Proofing Security:**

Investing in quantum-safe technologies now ensures that organizations are prepared for future threats. This proactive approach helps maintain trust with customers and stakeholders by demonstrating a commitment to long-term data security.

Quantum Safe Network – Multiple Options

Quantum Key Distribution (QKD)



- Hardware based
- Uses photon properties to generate secure keys
- Limited range (for now)
- Point-to-Point (for now)

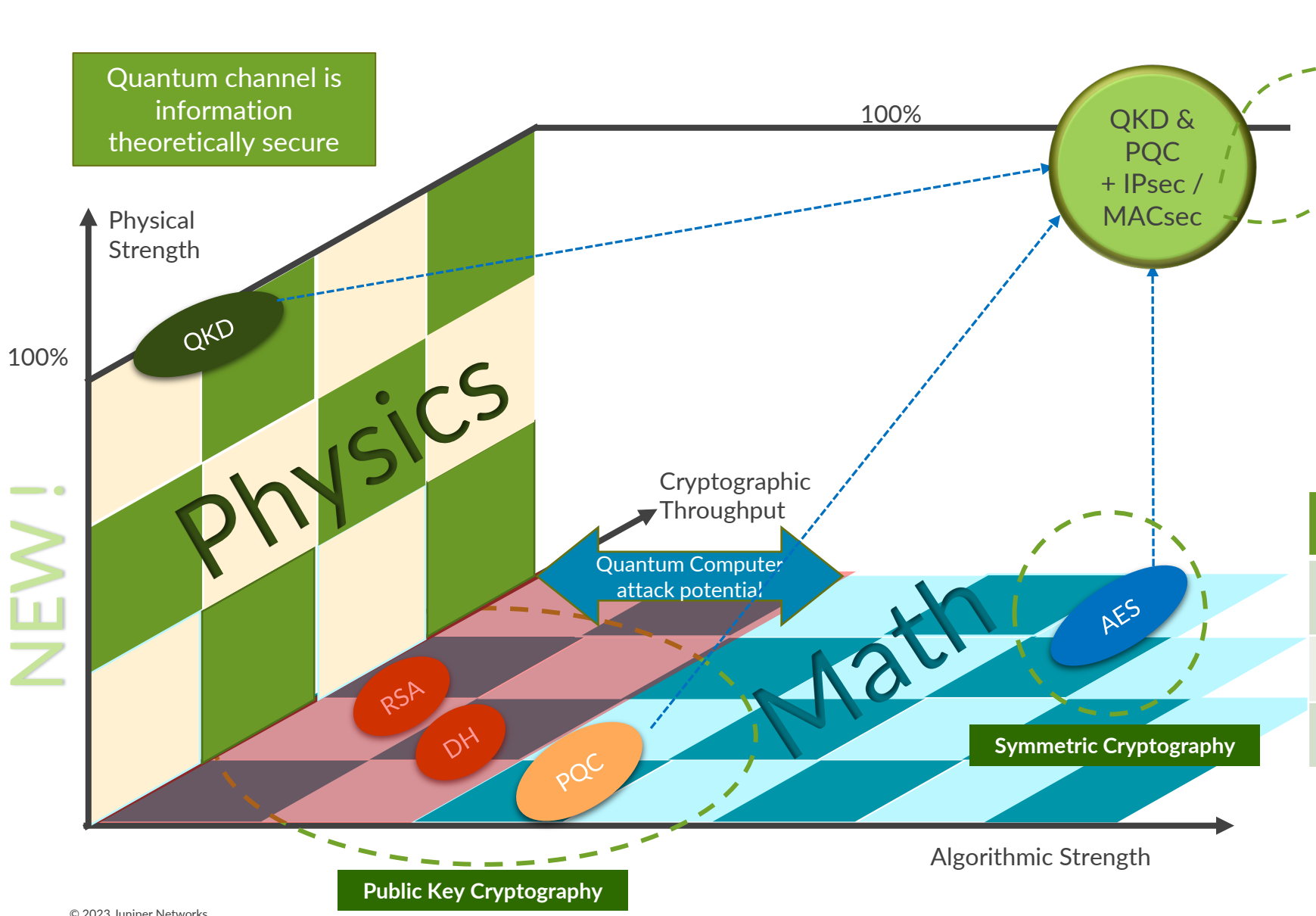
Post-Quantum Cryptographic (PQC) Algorithms

- Standardization of new 'quantum resistant' crypto algorithms in the works
- Selection process ongoing

Quantum-safe tunnels

- Add an additional secret to symmetric key material based on long random number
- Standards based for quantum key use (RFC8784) and key delivery (ETSI-014)

How does Quantum Technology Differentiate?



Quantum Secured Tunnel

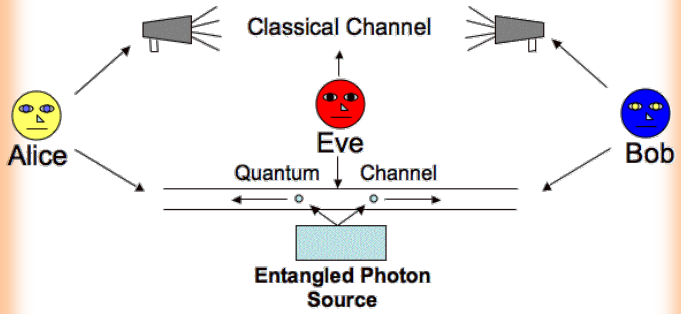
Quantum Secured IP/MPLS Infrastructure

QKD is one of multiple security enhancement investments being made across the industry to prevent the risk of Quantum Computing being used by malicious adversaries

	sharing	Crypto Engine	Entropy Source
Public crypto (RSA, DH)	Public key	Math	Local RNG
Symmetric (AES)	Private key	Math	from local RNG or QKD
QKD	none	Physics	Quantum-RNG

Quantum Safe Network - QKD

Quantum Key Distribution (QKD)



- Hardware based
- Uses photon properties to generate secure keys
- Limited range (for now)
- Point-to-Point (for now)

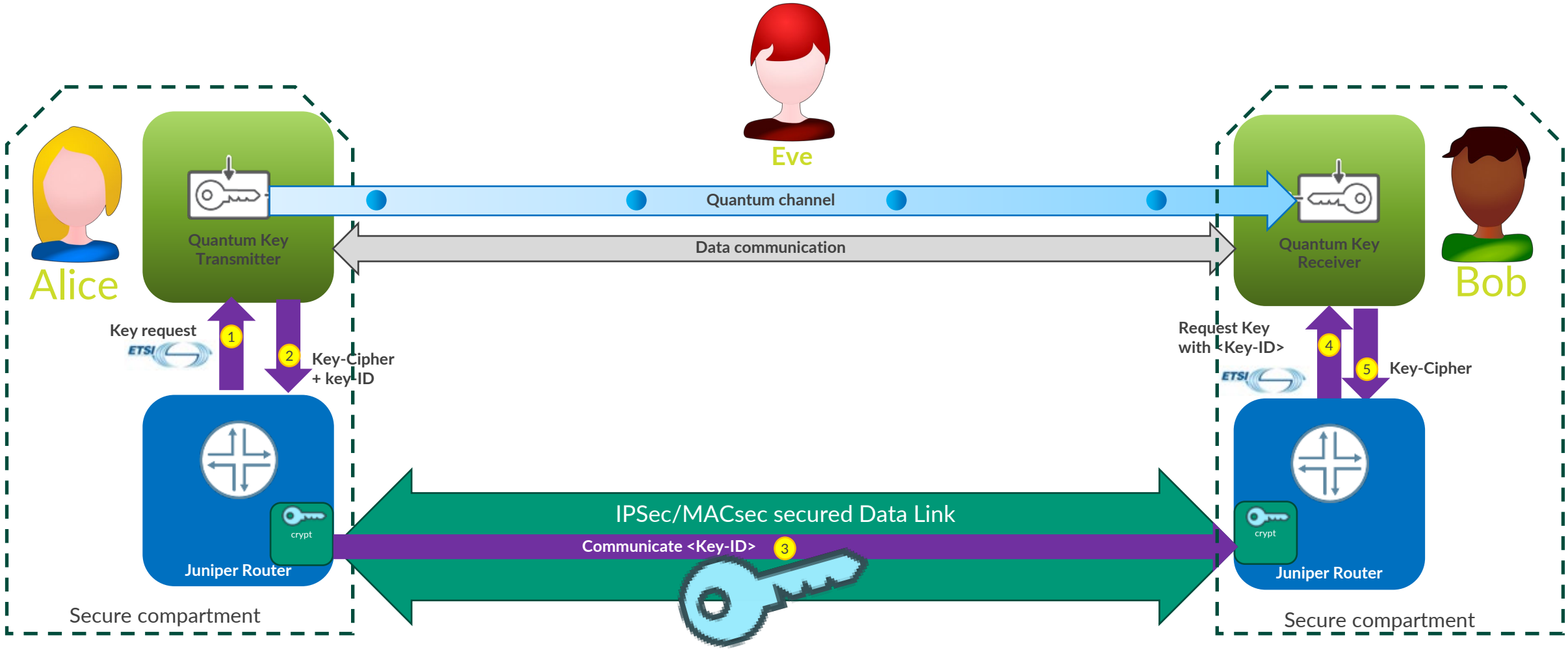
Quantum Key Distribution (QKD) is a secure communication method that uses the principles of quantum mechanics to generate and distribute cryptographic keys. It allows two parties to produce a shared, random secret key known only to them, which can then be used to encrypt and decrypt messages.

One of the key features of QKD is its ability to detect any hacking attempts. If a third party tries to intercept the key, the quantum state of the particles used to transmit the key will be disturbed, alerting the parties.

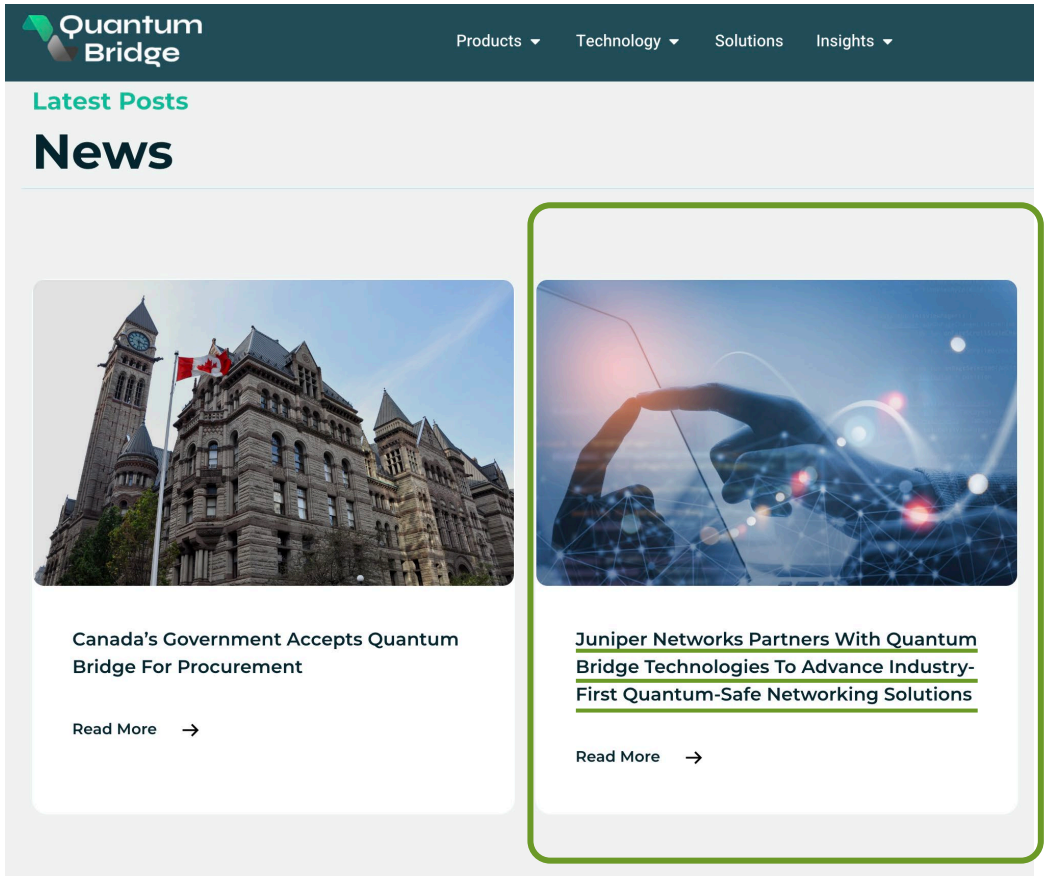
This makes QKD an extremely secure method for key distribution

Quantum-Safe IPsec/MACsec

Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API ETSI GS QKD 014



Quantum Bridge invesment



FINANCIAL TIMES

HOME WORLD US COMPANIES TECH MARKETS CLIMATE OPINION LEX WORK & CAREERS LIFE & ARTS HTSI

MARKETS › MARKETS DATA › EQUITIES | Equities Screener Sectors & Industries Company Announcements Director Dealings Worl

Company Announcements

Juniper Networks Inc

Juniper Networks Partners with Quantum Bridge Technologies to Advance Industry-First Quantum-Safe Networking Solutions

AUG 28 2024 12:45 BST

Juniper Ventures makes security investment to evolve Juniper's AI-Native Networking portfolio ahead of quantum computing threats

SUNNYVALE, Calif.--(BUSINESS WIRE)--Aug. 28, 2024-- Juniper Networks (NYSE: JNPR), a leader in secure, AI-Native Networking, today announced a strategic investment in Quantum Bridge Technologies, an industry leader in Distributed Symmetric Key Exchange (DSKE) for post-quantum cryptography (PQC) networks. This investment showcases Juniper's commitment to advancing quantum-safe communications by enabling Quantum Bridge to further scale its DSKE solution. To further inform ongoing research and product development in the field, the two companies will collaborate through Juniper Beyond Labs' pathfinding projects.

Customer Interest and Engagement 2023/24

verizon

AT&T

aws

eurofiber

Singtel

LIBERTY GLOBAL

BT

amsix

BANCA D'ITALIA

Canada

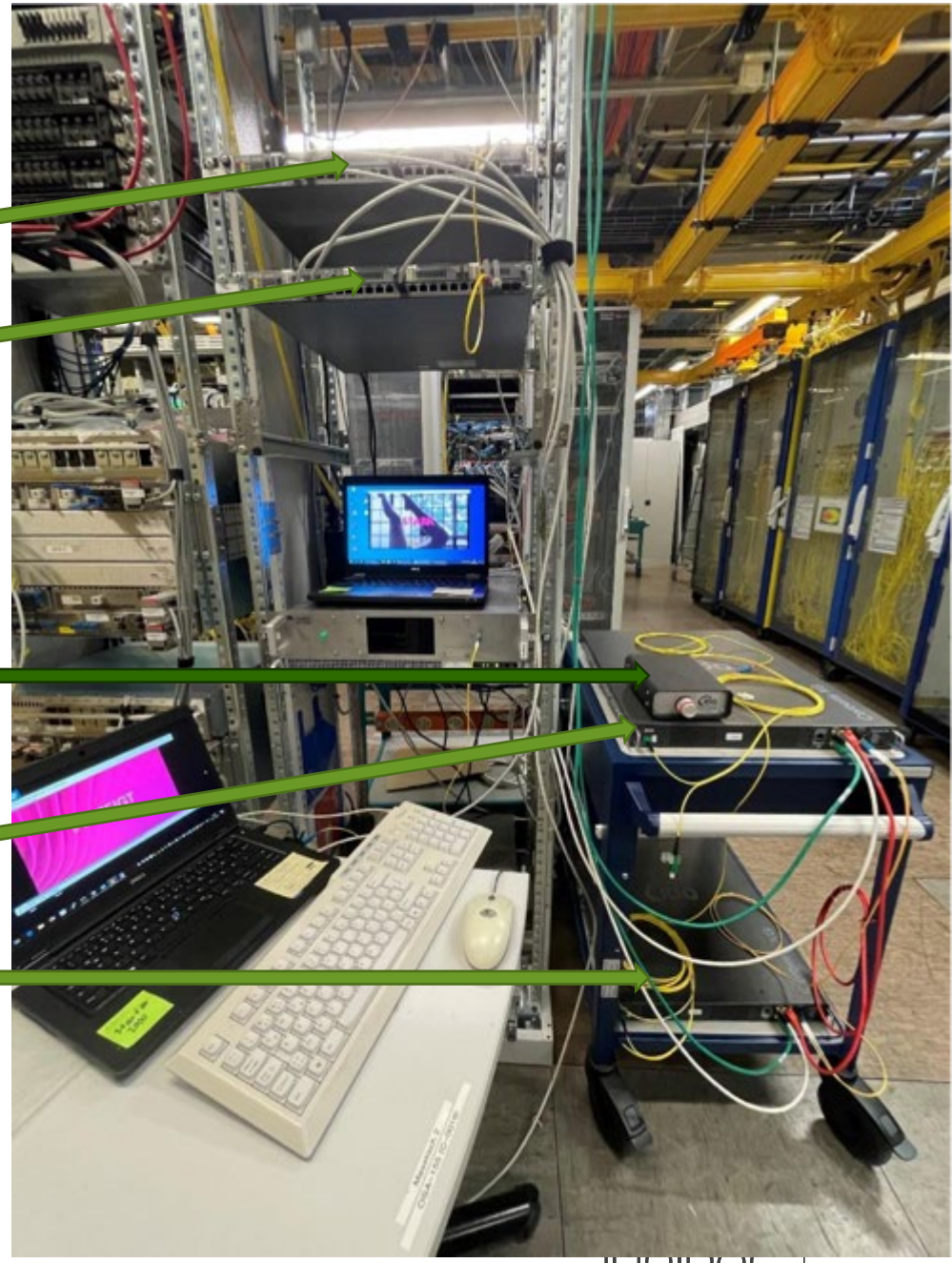
orange™

Quantum Cryptography

Alice and Bob
2* Juniper SRX380
MACsec @ 10G

Eavesdropping simulation device

QKD-Tx & QKD-Rx



Conclusion

As we journey toward the quantum internet, we must embrace these innovations and prepare our infrastructures to integrate quantum solutions. The road ahead is challenging. Together, we can build a future where our networks are not just secure, but quantum-secure.

THANK YOU

JUNIPER NETWORKS | Driven by Experience™