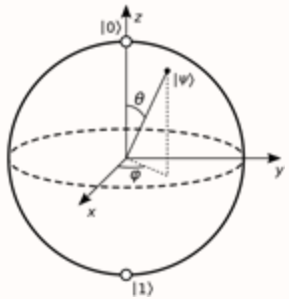
Qubits at the Gate: Superpositioning cybersecurity against quantum threats

Mel Mudin



MyNOG12
Malaysia Network Operators Group

Mel Mudin, CISO, PayNet

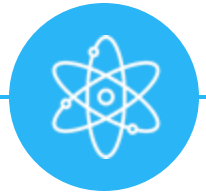
Current role

- Cybersecurity risk management
- Technology risk management
- Data security and protection
- R&D in the impact of AI and quantum computing on cyber

Background

- Cybersecurity consulting in Big 4
- B Sc. Electrical Engineering
- 20+ years in cybersecurity

Today’s topic is on the threats of quantum computing to cybersecurity, and the unified approach to collaboratively mitigate the threats

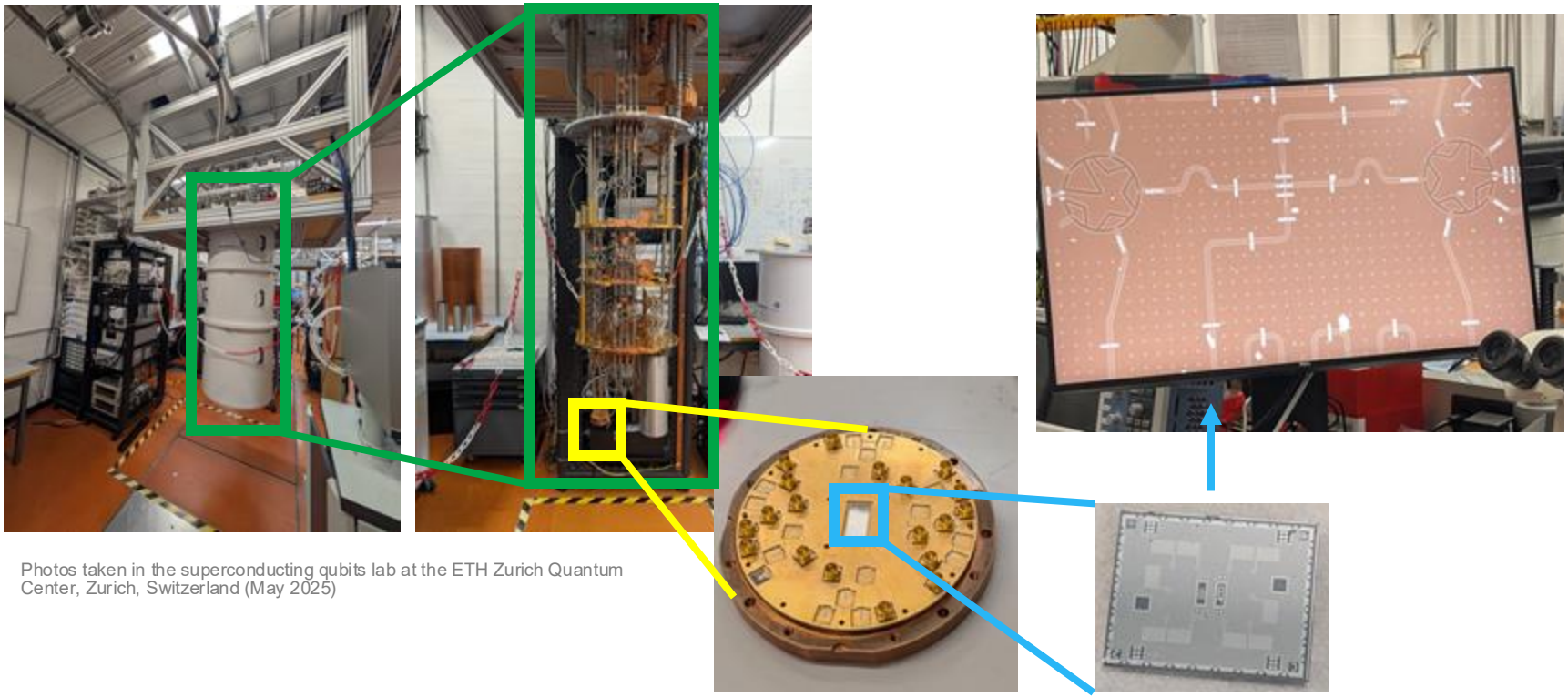


Quantum computing threats to classical cryptography

Risk mitigation approaches

A collaborative and unified approach for risk mitigations

Superconducting qubits is one of the many types of quantum computers

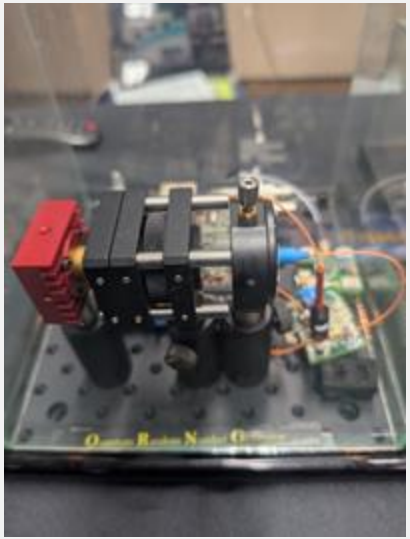


Photos taken in the superconducting qubits lab at the ETH Zurich Quantum Center, Zurich, Switzerland (May 2025)

Many quantum-based systems exist today

Quantum Key Distribution Hardware

SDT Inc



Quantum Random Number Generator

MIMOS

Photos taken from MIMOS Quantum Day in February 2025

The race to quantum supremacy is ramping up

Governments and global tech giants compete in the race for quantum supremacy, introducing breakthroughs in processors and error corrections that could scale commercially

Microsoft's Topological Breakthrough

Majorana 1 processor

World's first topological qubit-powered processor

Error protection

Topological approach shields qubits from environmental noise

Stability advantage

More stable than superconducting qubits

Google's Willow Error Correction Revolution

Exponential error correction

Revolutionary approach for error correction

Advanced architecture

Novel qubit arrangement enhances computational stability

Processing breakthrough

Enables more complex quantum algorithm than ever before

China's Quantum Advancements

Zuchongzhi-3 chip

China's flagship quantum computer

Speed claims

Reportedly outperform's Google's processors

Global competition

Positions China as a quantum computing leader

1000+	100x	99.9%
Qubits in the latest generation processors	Speed improvement over previous quantum generations	Error corrections goal for commercial viability

Major cloud providers, quantum technology leaders, and niche players already provide quantum-as-a-service

Quantum-as-a-service (QaaS) democratizes access to quantum computing. Major cloud providers, big tech, and specialized startups are leading this technological revolution

IBM Q Experience
Offers access to real quantum devices and simulators through Qiskit

Google Quantum AI
Provides cloud-based quantum computing through Cirq software library

AWS Braket
Enables quantum programming and access to quantum computers and simulators

Azure Quantum
Integration of Microsoft Azure with quantum hardware, software, and services

WHAT IS THE THREAT?

The impact of quantum algorithms on classical cryptography

Quantum algorithms are challenging the foundations of modern security systems and reshaping our approach to encryption

Shor's Algorithm (1994)

Solves the integer factorization problem (IFP) which is used by public key cryptography

N = pq
35 = ? X ?

Quantum computer can solve this problem in hours

Complete compromise of RSA and other public key cryptographic systems

RSA & elliptic curve cryptography
Diffie-Hellman key exchange
Digital signatures

Grover's Algorithm (1996)

Provides quadratic speedups for unstructured search algorithm (makes brute force faster)

Reduces the security strengths of symmetric encryption systems

AES
SHA

Further reading:
https://www.ibm.com/quantum/blog/factor-15-shors-algorithm
https://www.nature.com/articles/s41598-021-95973-w

Future outlook and current status

21

Largest number
Factored by Shor's algorithm as of 2023

<1

Million qubits
Estimated number of qubits to break RSA-2048[1]

5-15

Years
Estimated timeline for cryptographically relevant quantum computers

Harvest Now, Decrypt Later

Collect data

Adversaries are harvesting encrypted traffic today. They can't decrypt it yet

Wait

Encrypted data is stored until quantum decryption becomes available

Decrypt later

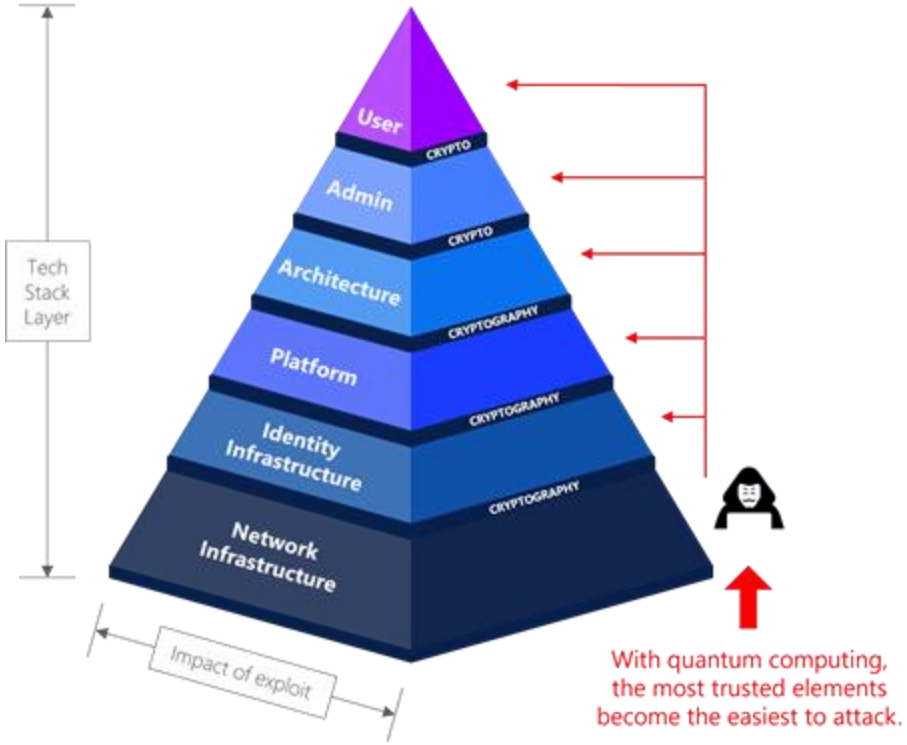
Once quantum computers mature, today's secrets become tomorrow's exposures

Today's concern

Data with long term-secrecy requirements is already at risk

1. How to factor 2048-bit integer with less than a million noisy qubit - https://arxiv.org/abs/2505.15917

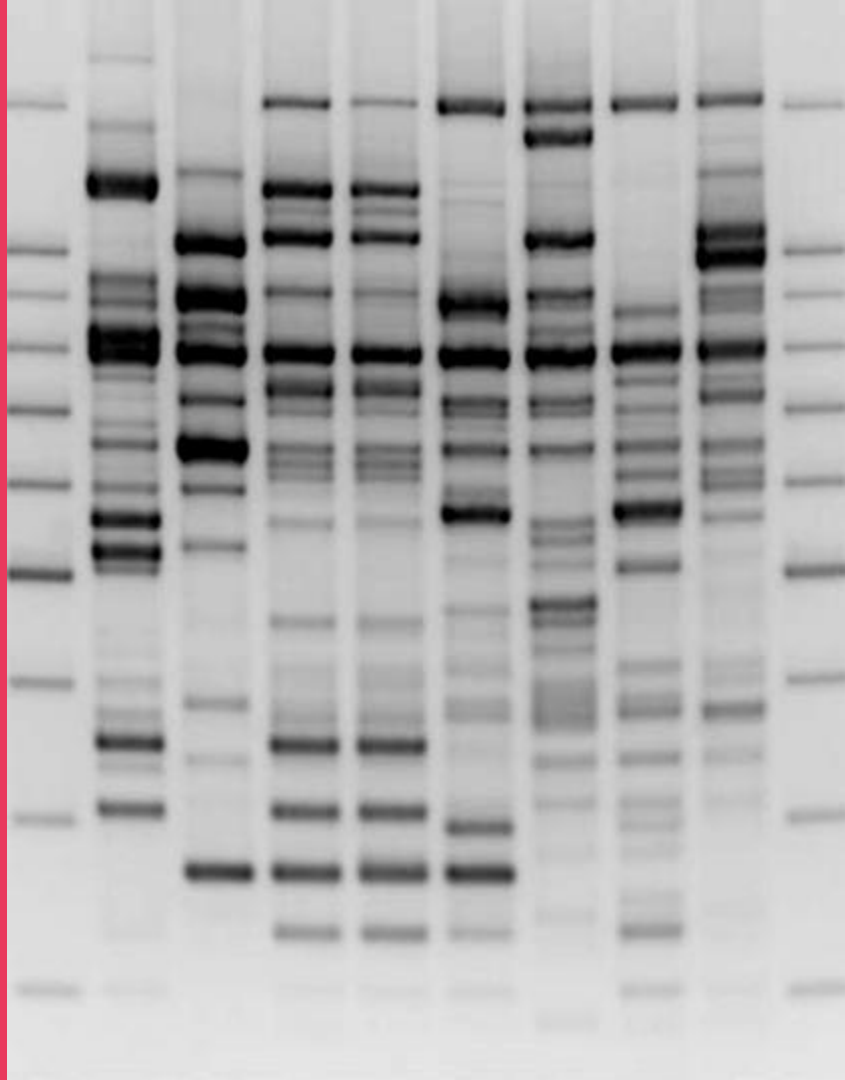
Harvest now, decrypt later threat inverts the typical cyber attack process



- Cryptography is integrated across all layers of the tech stack
- Cyberattacks typically begins at the top, and requires attackers to circumvent multiple layers of defense to get access to the core systems that hosts valuable data
- Quantum threats invert this process by tapping the network infrastructure layer

Source: ID Quantique

RISK MITIGATION APPROACHES



Two approaches: post-quantum cryptography (PQC) and quantum key distribution (QKD)

Post-quantum cryptography (PQC)

Quantum resistant algorithms

Believed to be hard for both classical and quantum computers

Multiple approaches

Lattice-based, hash-based, and code-based schemes

Standardization effort

NIST is leading global efforts to validate and certify algorithms

Strengths

- Software-based, works with existing infrastructure
- Immediate deployment possible
- Protects against harvest now, decrypt later

Limitations

- Not provably secure
- Not mature; long term development unclear
- May face new attack vectors

Two approaches: post-quantum cryptography (PQC) and quantum key distribution (QKD)

Quantum key distribution

Quantum mechanics

Uses fundamental physics for unbreakable key exchange

Eavesdropper detection

Any interception disturbs quantum states, revealing attacks

Provable security

Based on physics, not computational difficulty

Long term solution

Bridges the short-term risk of PQC and is the most secure long-term solution

Limitations

Infrastructure and deployment challenges

Requires specialized hardware, availability of dark fiber, and may be susceptible to noise

Scalability and network limitations

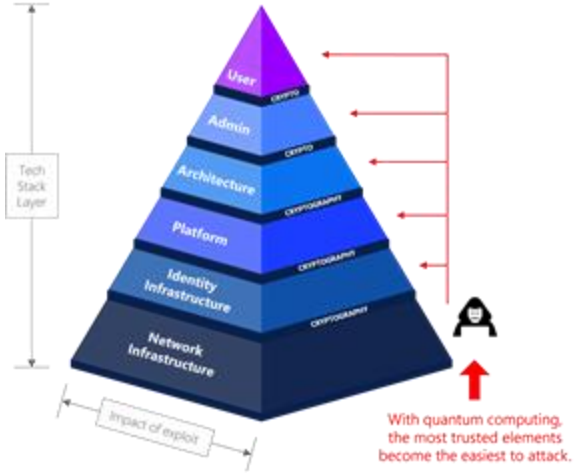
Multi-party networks get complex to implement

Cost and implementation obstacles

Specialized hardware cost; potentially high maintenance cose

PQC migration: anticipating a lengthy and complex process with unforeseen business impacts

Visibility challenges



Requires greater visibility of how and where cryptography is currently being used

Time and resource constrains

Auditing all cryptographic elements (libraries, certificates) is lengthy, complex, and costly, so migration timelines will vary significantly by asset

Repeated migration risk

There is a likelihood that migration needs to be repeated with the release of newer cryptographic standards

Implementing PQC won't happen overnight as cryptography is typically not managed as a strategic asset; anticipate a long, complex, and iterative process; steps required to migrate may take decades or more, moving the acceptable risk well into the quantum threat horizon

Other key considerations for migration

Performance Impact	PQC requires more computational resources and larger key sizes; impacts memory-constrained hardware and increases bandwidth
Interoperability	Upgrades may scatter over time; a single non-upgraded system can create bottlenecks; PQC upgrades must happen in sync across all systems
Standardization & Regulatory Guidance	PQC adoption hinges on mature standards and regulatory guidance
Cost & Resource Allocations	Cost and resource intensive exercise - may take years
Transition Challenges & Risks	New algorithms are not fully tested and deployed in real world; may introduce complex key management
Supply Chain Readiness	Vendors may wait for finalized standards or regulatory guidance before investing in PQC upgrades

TURNING RISKS INTO OPPORTUNITIES

Turning risks into opportunity: Singtel quantum-safe network as a service

Singtel Quantum-Safe Network

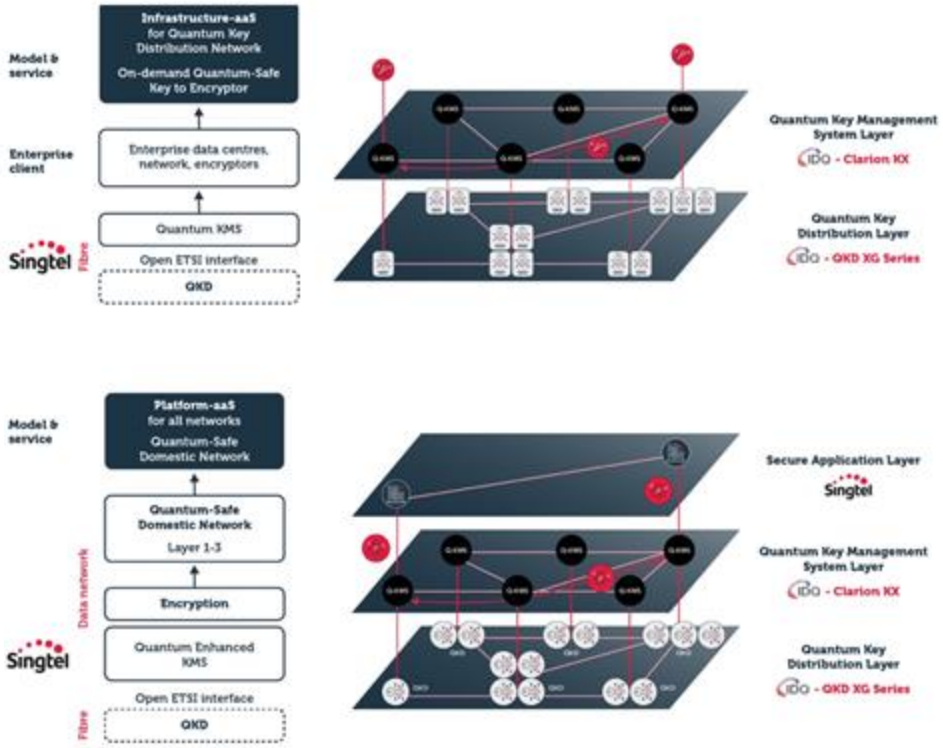
Southeast Asia's first National Quantum-Safe Network Plus (NQSN+)

Quantum Key as-a-Service (QK-aas)

Leverages QKD and PQC

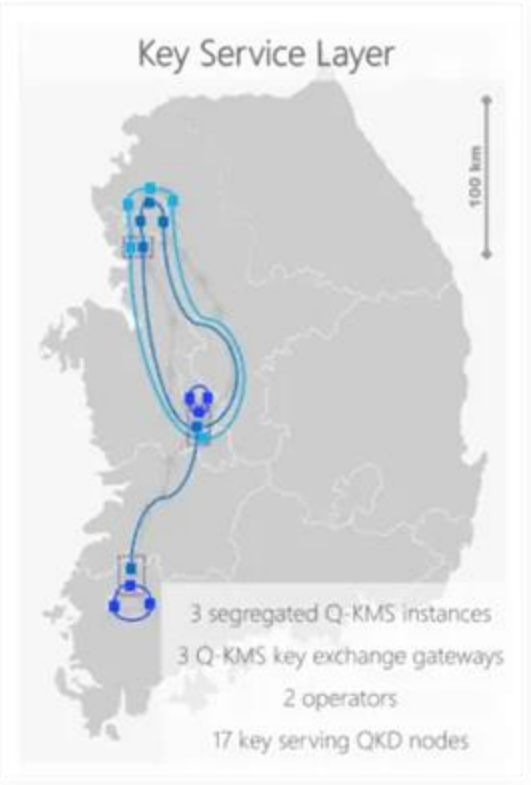
Fully managed network and infrastructure

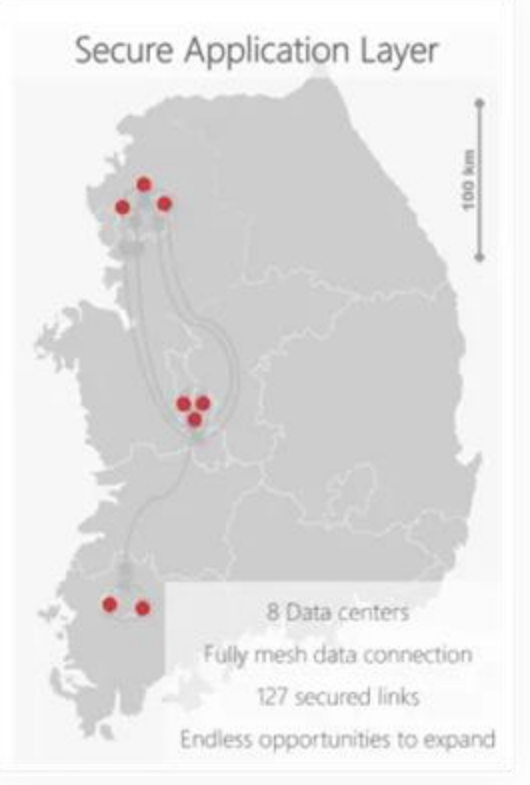
Service-based model with managed services



Source: Singtel, ID Quantique

Turning risks into opportunity: South Korean quantum safe key distribution (QKD) network

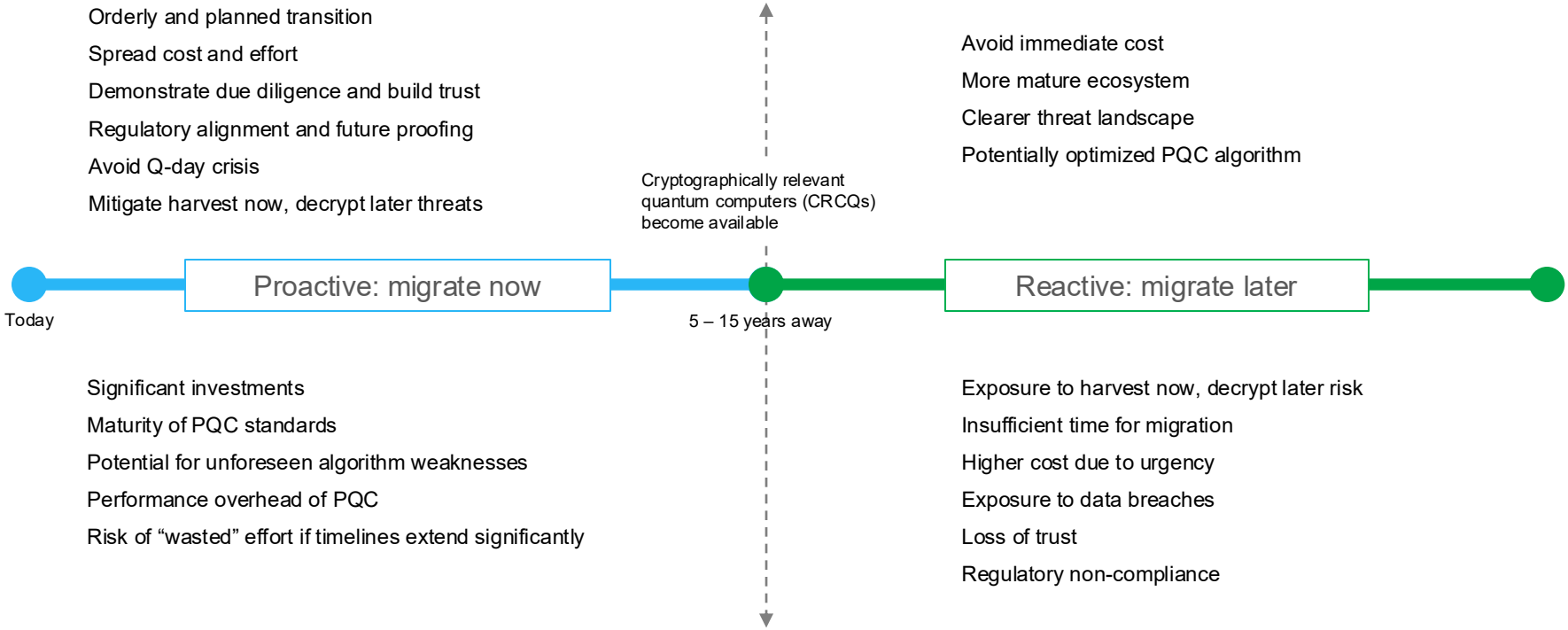




Source: https://www.idquantique.com/quantum-safe-security/nation-wide-quantum-safe-key-distribution-network-in-south-korea/

NEXT STEPS

While cryptographic threat is fairly well-defined, the exact timing of when the threat will materialize is unclear: act now or wait?



A unified and collaborative approach is required to strengthen the resiliency of the telco and financial ecosystem

- Set the (national) standard for PQC
- Develop an industry strategy and approach for migration
- Determine crypto standards and requirements for the procurement of hardware, software, and services
- Build capabilities for discovery, inventory, and risk assessment

Let’s collaborate! Reach out to me if you want to take part in building a secure Malaysia

THANK YOU!