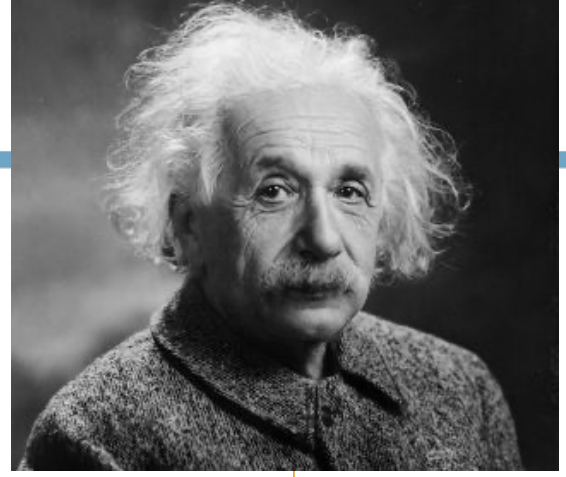
TNO innovation for life

QUANTUM SECURITY

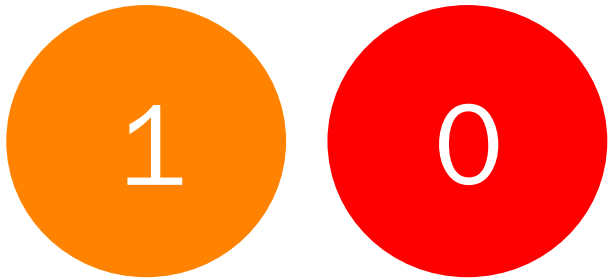
DRS IR MARAN VAN HEESCH

maran.vanheesch@tno.nl

QUBITS



Superposition



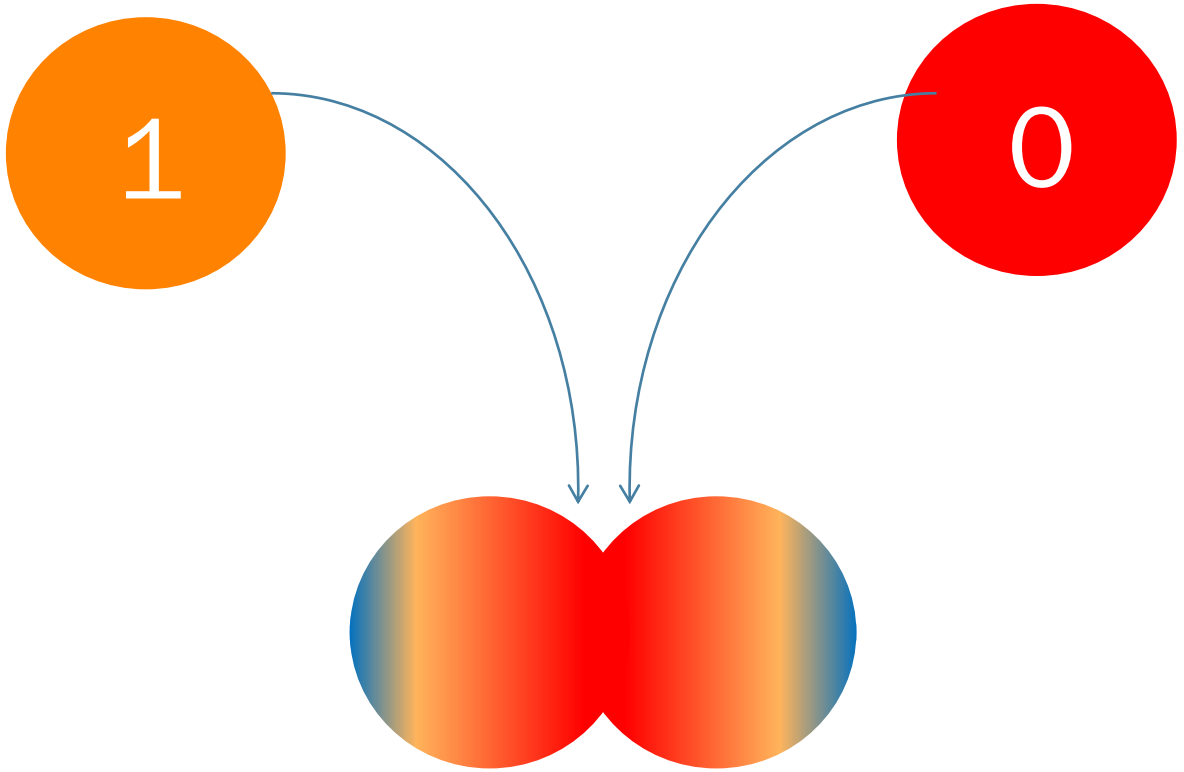
State of particle:

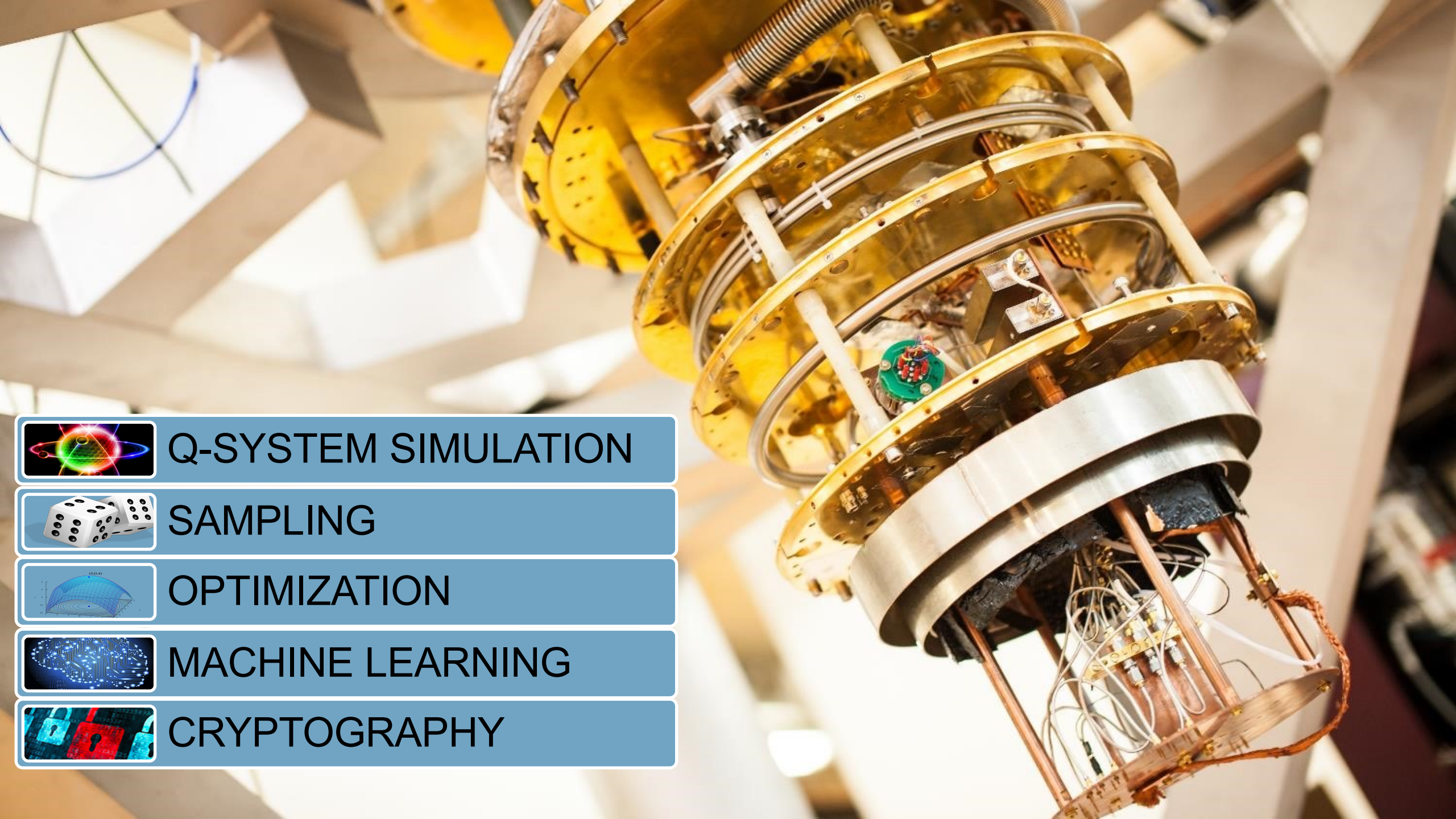
0 (up) **or** 1 (down)

State of particle:

0 (up) **and** 1 (down)

Entanglement




Q-SYSTEM SIMULATION
SAMPLING
OPTIMIZATION
MACHINE LEARNING
CRYPTOGRAPHY

The Economist | Topics | Current edition | More

Future-proofing the internet

Quantum computers will break the encryption that protects the internet

Fixing things will be tricky

Print edition | Science and technology ›

Oct 20th 2018

Broken:
RSA
ECC
DH

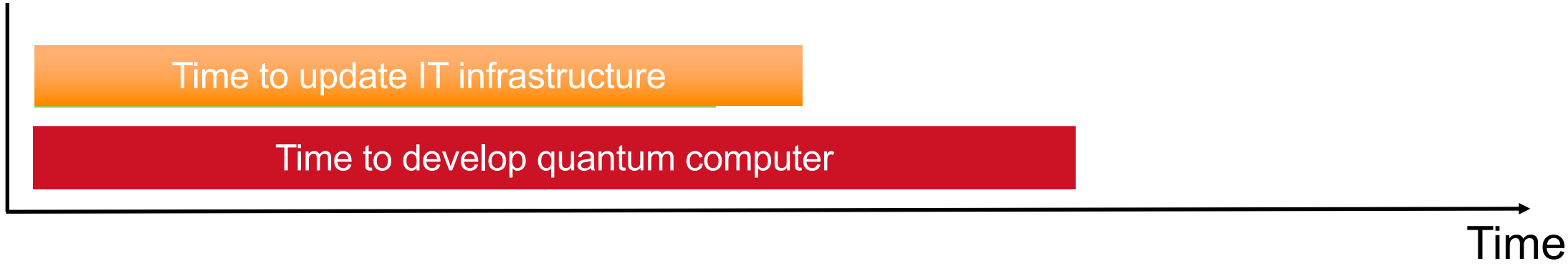
Weakend:
AES

QUANTUM TECHNOLOGIE MOET NU AL MEEGENOMEN WORDEN IN IT-AUDITING

- A: Eens
- B: Oneens

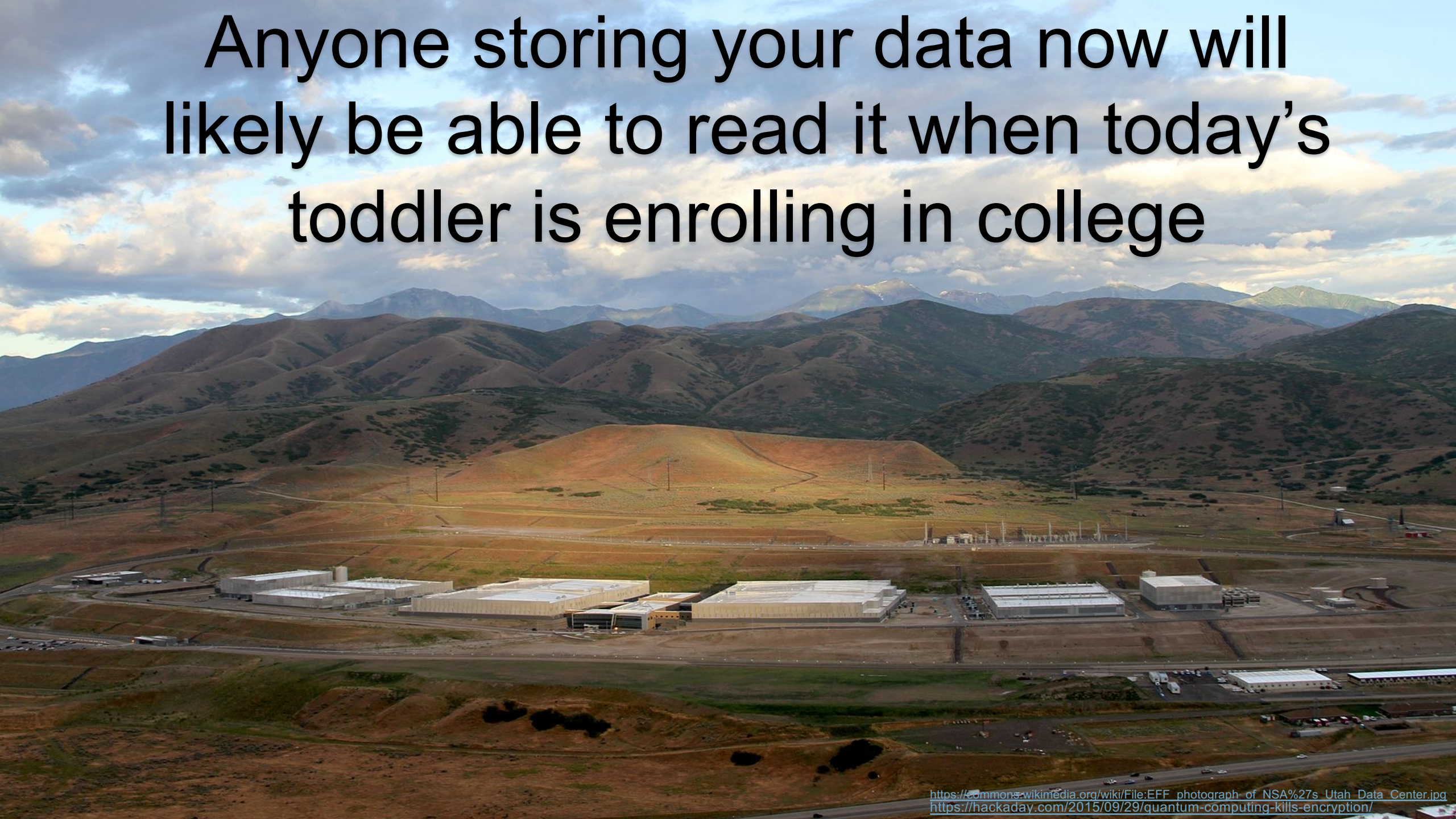
NOREA - de beroepsorganisatie van IT-Auditors

WHY START NOW?



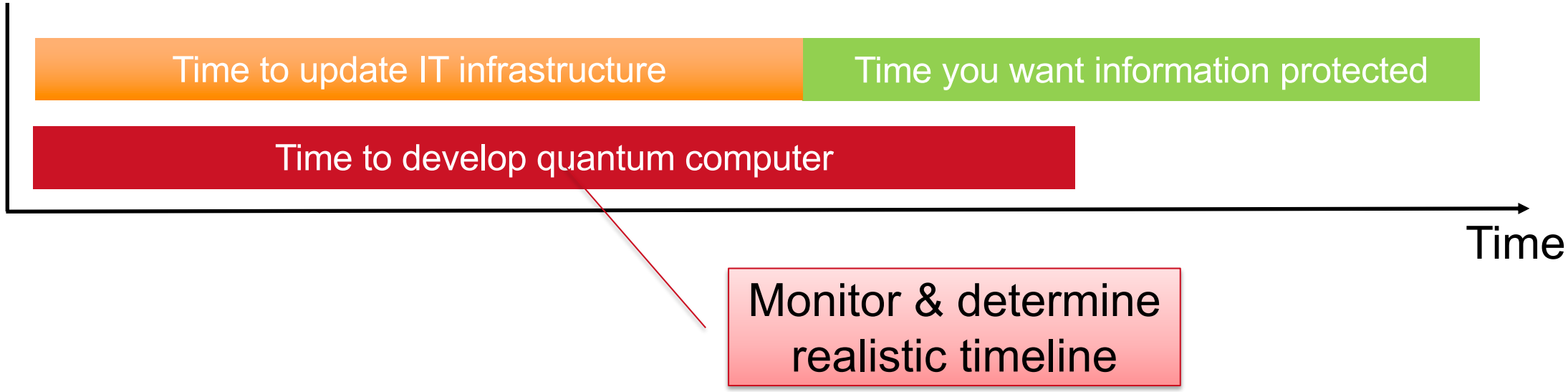
https://globalriskinstitute.org/publications/quantum-threat-timeline/

Anyone storing your data now will likely be able to read it when today's toddler is enrolling in college



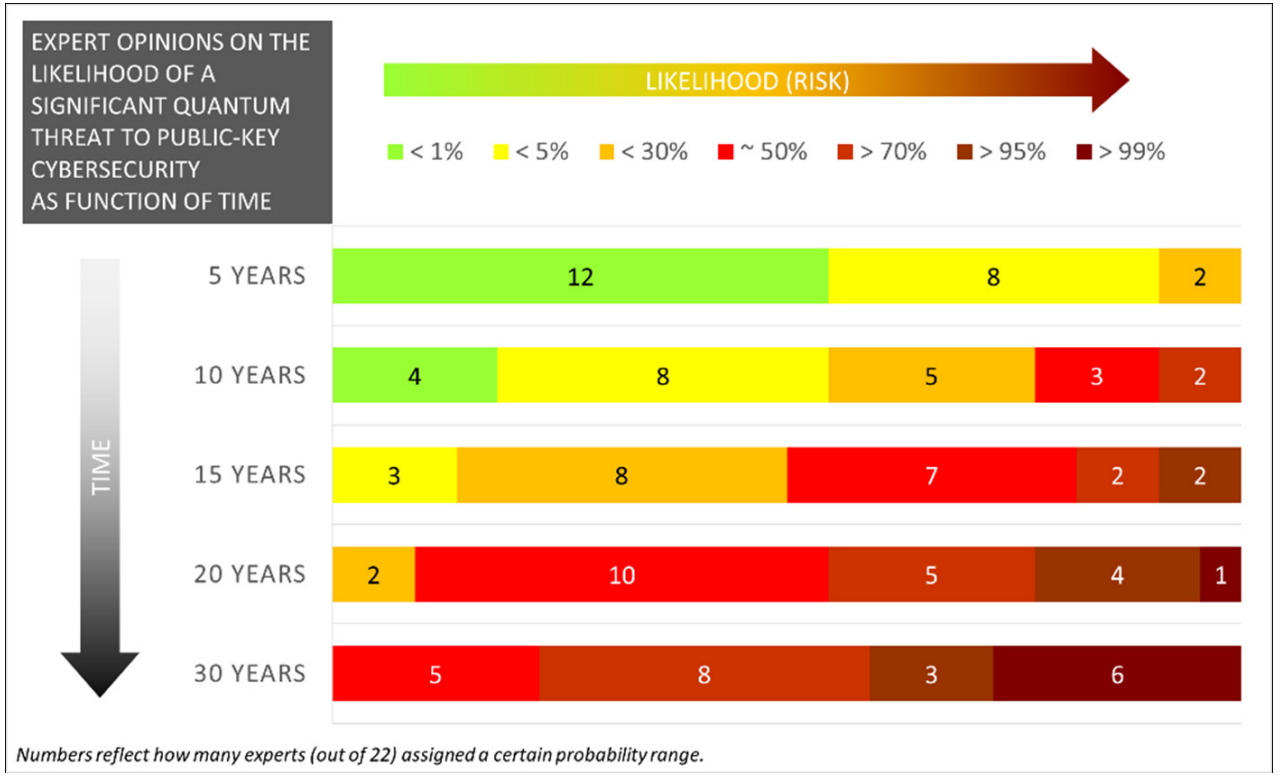
https://commons.wikimedia.org/wiki/File:EFF_photograph_of_NSA%27s_Utah_Data_Center.jpg
https://hackaday.com/2015/09/29/quantum-computing-kills-encryption/

WHAT CAN YOU DO?



https://globalriskinstitute.org/publications/quantum-threat-timeline/

AN EXPERT VIEW



https://globalriskinstitute.org/publications/quantum-threat-timeline/

WHAT ARE CURRENT QUANTUM COMPUTERS CAPABLE OF?

tweakers

Zoek naar nieuws

hosted by TRUE

IBM wil in 2023 quantumprocessor met 1000 qubits gereed hebben

Door **Olaf van Miltenburg**
Nieuwscoördinator
Feedback • 16-09-2020 11:44 58 • submitter: TheVivaldi

IBM werkt aan drie quantumprocessors die in de komende drie jaar moeten verschijnen. In 2023 hoopt het bedrijf de mijlpaal van meer dan duizend qubits behaald te hebben. Dat moet gebeuren met de Condor-processor.

IBM Quantum Computing heeft een naar eigen zeggen agressieve roadmap opgesteld voor zijn plannen om quantumsystemen op te schalen. Het bedrijf nam deze maand stilletjes de Hummingbird in gebruik: een quantumprocessor met 65 qubits. Een van de eigenschappen hiervan is dat het bedrijf signalen van acht qubits in een keer kan uitlezen.

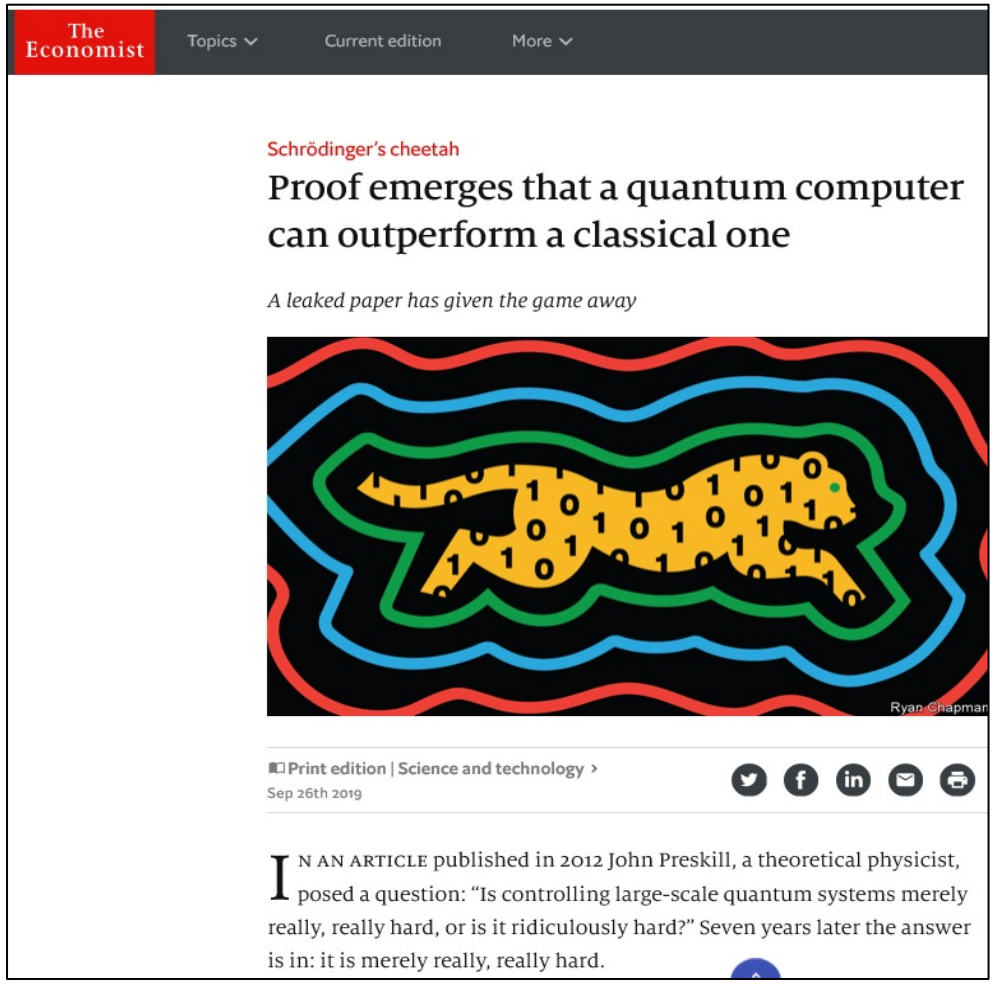
65 qubits

D-Wave's 5,000-qubit quantum computing platform handles 1 million variables

Emil Protalinski @EPro September 29, 2020 7:45 AM Dev

5000 qubits

WHAT ARE CURRENT QUANTUM COMPUTERS CAPABLE OF?



The Economist Topics Current edition More

Schrödinger's cheetah

Proof emerges that a quantum computer can outperform a classical one

A leaked paper has given the game away

Ryan Chapman

Print edition | Science and technology ›
Sep 26th 2019

IN AN ARTICLE published in 2012 John Preskill, a theoretical physicist, posed a question: "Is controlling large-scale quantum systems merely really, really hard, or is it ridiculously hard?" Seven years later the answer is in: it is merely really, really hard.

Breaking RSA

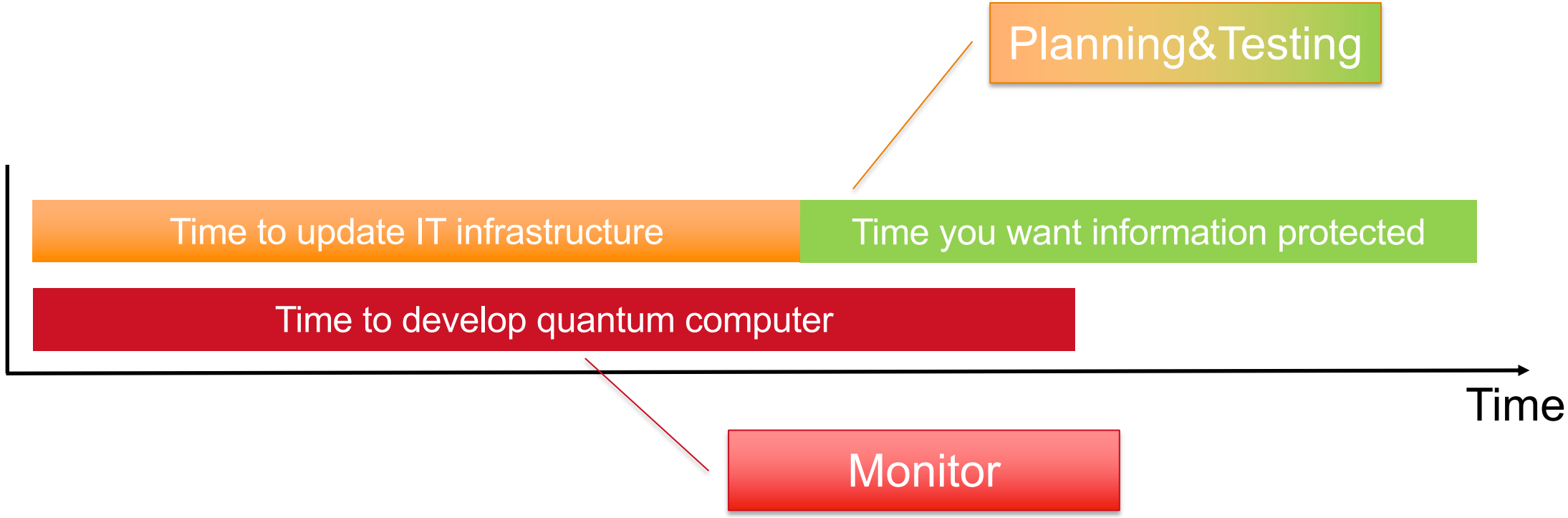
Classically
RSA-768
2010

IBM Q
35 (6 bits)
2019
7 qubits

D-Wave 2000Q
1005973 (20 bits)
2019
89 qubits

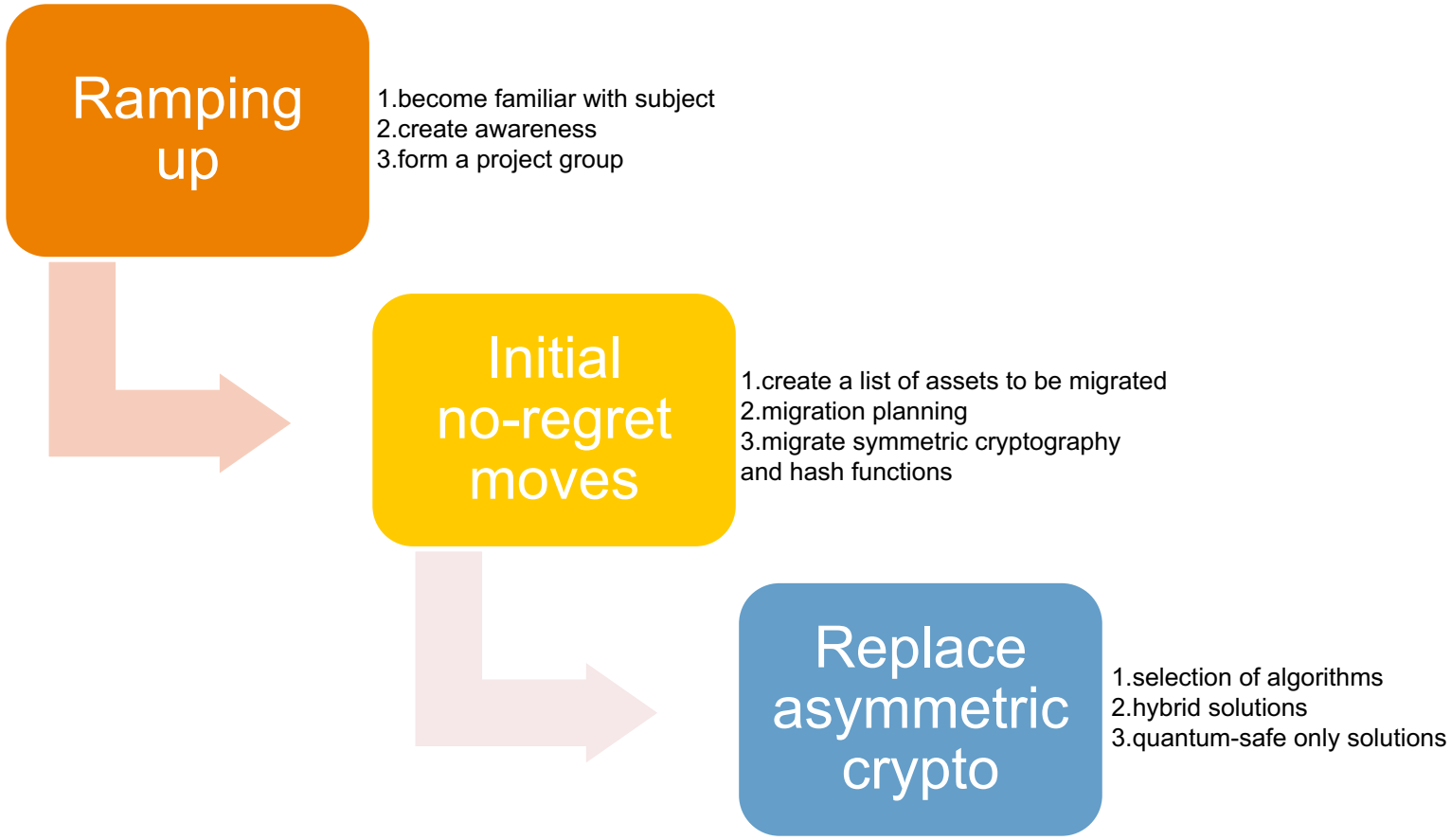
Does not use Shor's algorithm

WHAT CAN YOU DO?



https://globalriskinstitute.org/publications/quantum-threat-timeline/

MIGRATION PLAN

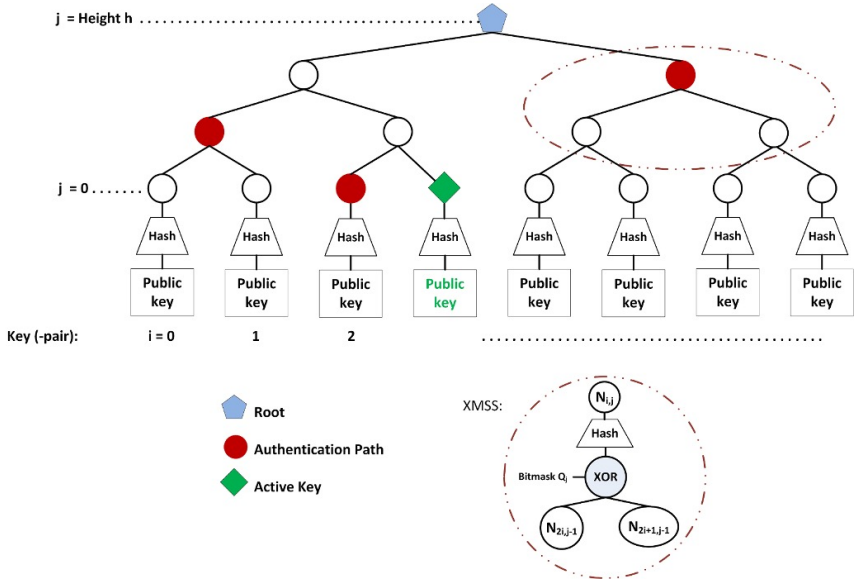


QUANTUM-SAFE ALTERNATIVES

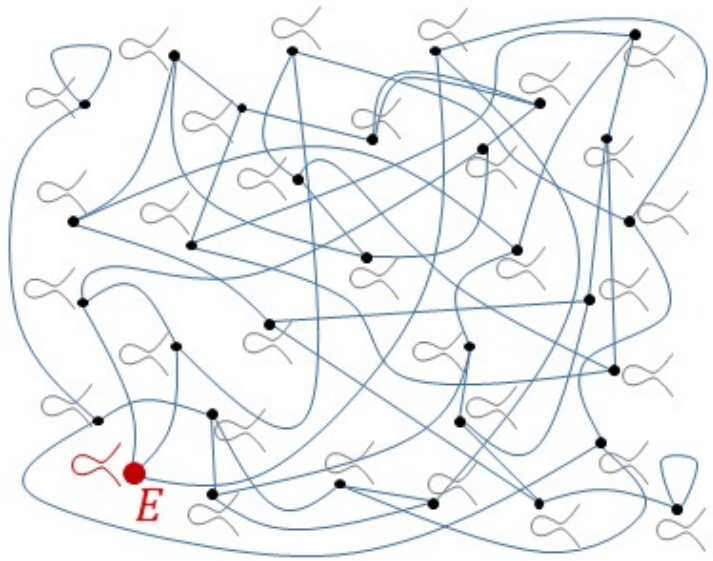
Challenge	(often used) Cryptographic solution	Currently used cryptographic protocol	Non-cryptographic solution
Data encryption	Symmetric cryptography	AES	-
Key exchange	Asymmetric cryptography	Post-quantum cryptography, QKD	Trusted courier, face-to-face meeting
Authentication & Integrity	Asymmetric cryptography	Post-quantum cryptography	Face-to-face meeting
Efficiency (building block)	Cryptographic hash functions for efficiency	SHA-2	-

POST-QUANTUM CRYPTOGRAPHY

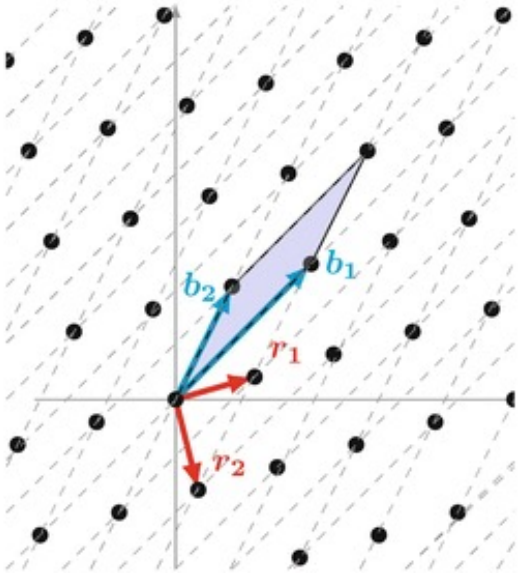
- Need to ***diversify*** the cryptographic protocols and associated mathematical problems.
- Protocols also vary in performance



Hash-based



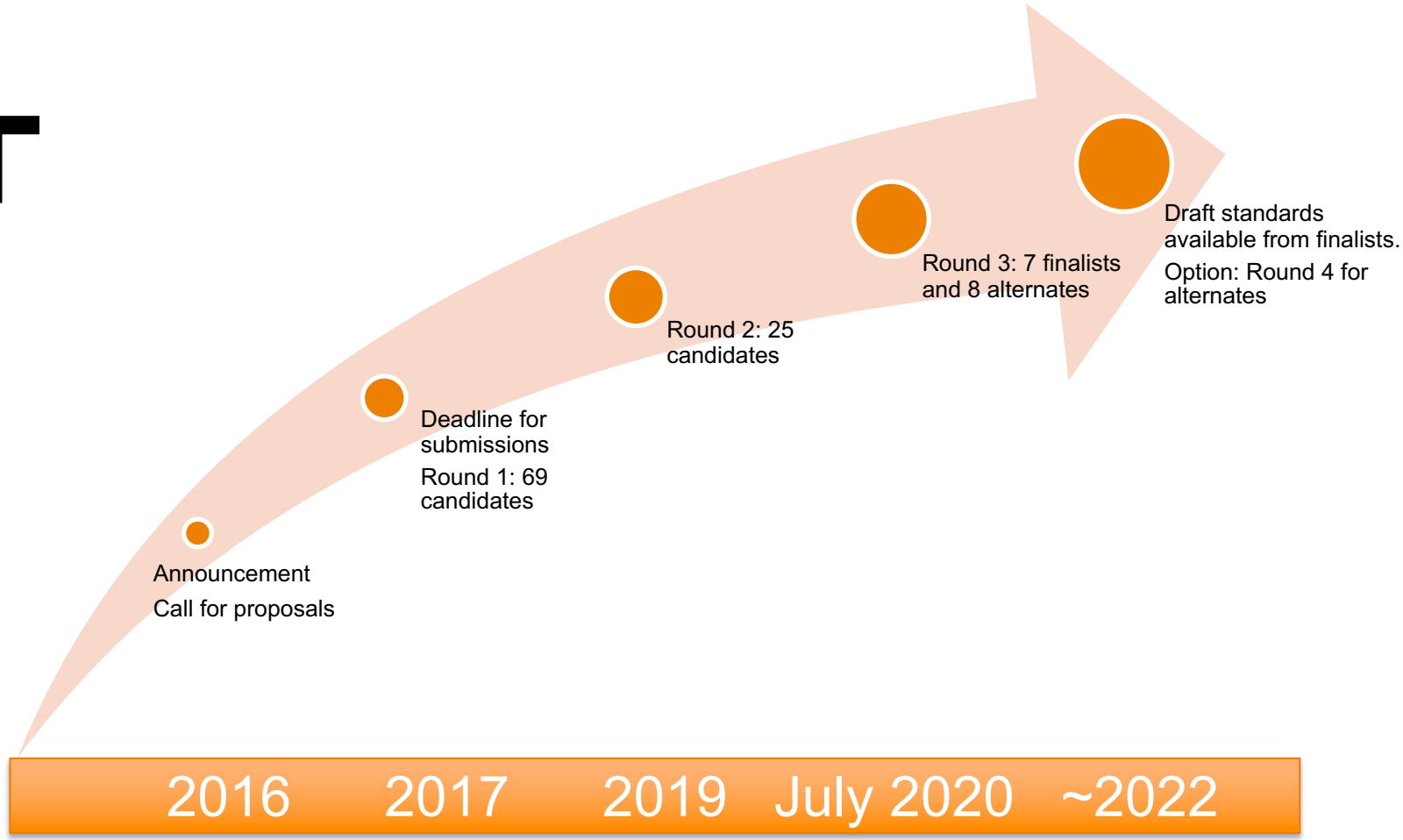
Supersingular Isogenies



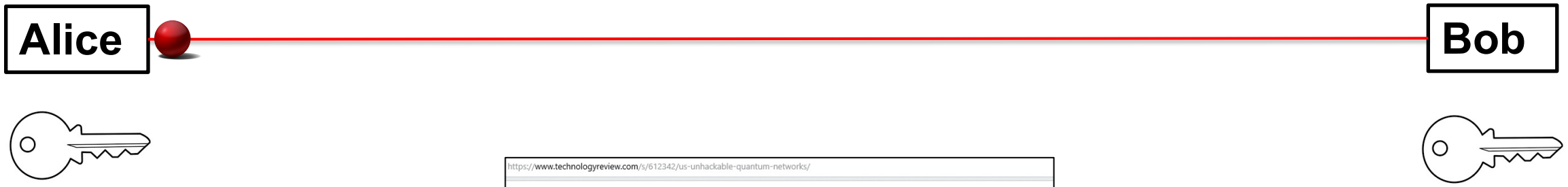
Lattice-based

Figure: https://www.esat.kuleuven.be/cosic/elliptic-curves-are-quantum-dead-long-live-elliptic-curves/

STANDARDISATION: NIST



QUANTUM KEY DISTRIBUTION (QKD)



- Promise: Inherent security

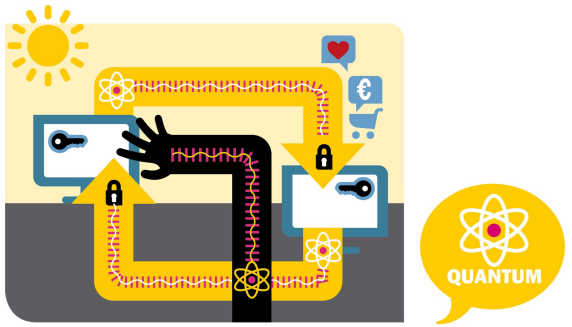
https://www.technologyreview.com/s/612342/us-unhackable-quantum-networks/

Connectivity

The US is finally getting a hacker-proof quantum network that people can use

The fiber-optic cables carrying data across the internet are vulnerable. Two US initiatives aim to fix that by creating super-secure quantum transmissions.

by Martin Giles October 25, 2018



Secure communication

Distributed computation

Syncing clocks

High resolution sensors

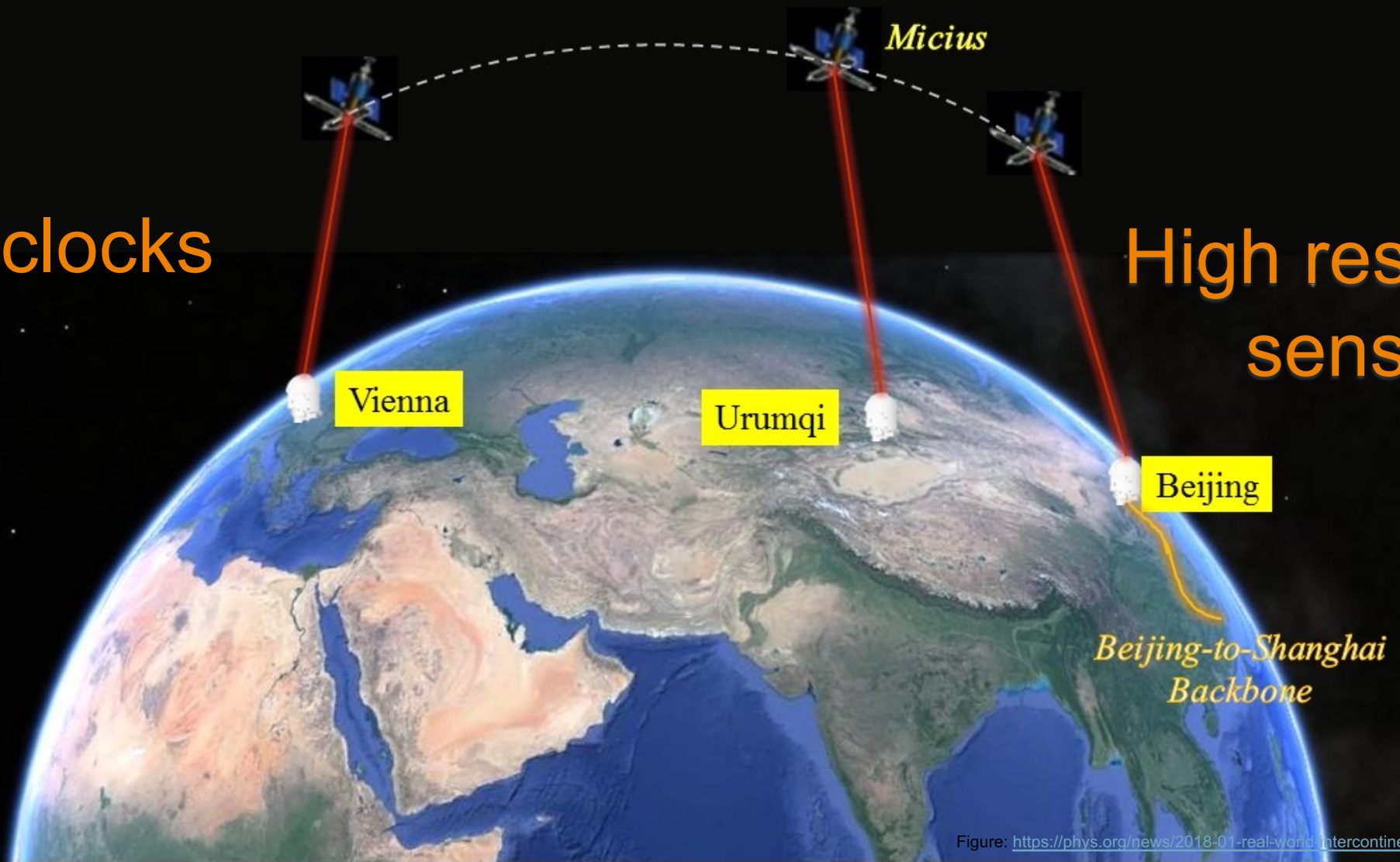


Figure: https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html

Schrödinger's cheetah

Proof emerges that a quantum computer can outperform a classical one

A leaked paper has given the game away

Print edition | Science and technology ›
Sep 26th 2019

IN AN ARTICLE published in 2012 John Preskill, a theoretical physicist, posed a question: "Is controlling large-scale quantum systems merely really, really hard, or is it ridiculously hard?" Seven years later the answer is in: it is merely really, really hard.

Future-proofing the internet

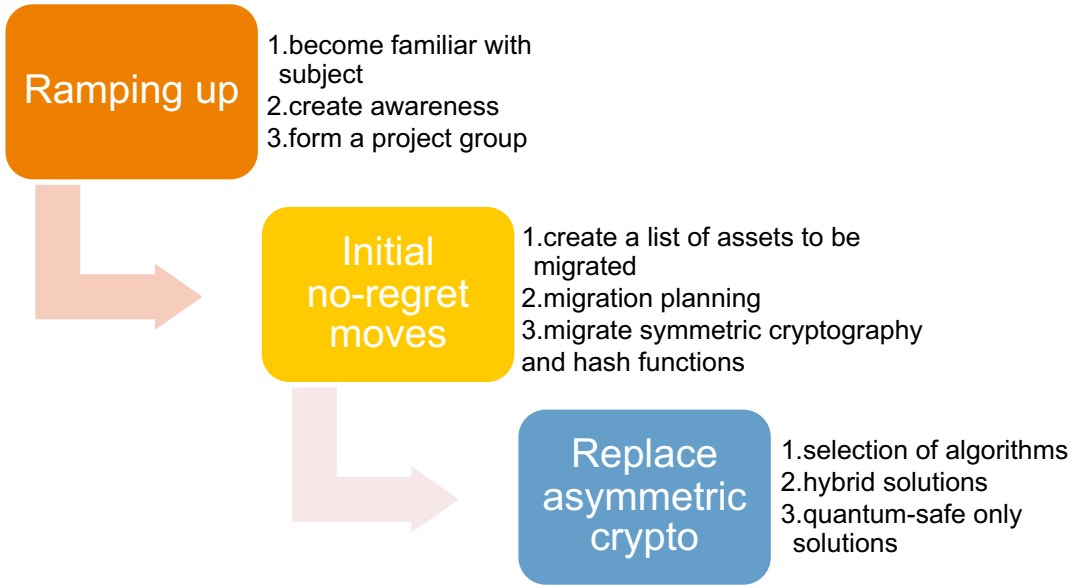
Quantum computers will break the encryption that protects the internet

Fixing things will be tricky

Print edition | Science and technology ›
Oct 20th 2018

WAT IS DE BELANGRIJKSTE ROL VOOR EEN IT-AUDITER IN HET MIGRATIE TRAJECT?

- A: Advisering van organisatie over de migratie
- B: Actief bijdragen aan de migratie
- C: Er is geen rol
- D: Anders, namelijk ……



QUANTUM FLAGSHIP

Discover Understand Engage Participate

The future is Quantum.

The Second Quantum Revolution is unfolding now, exploiting the enormous advancements in our ability to detect and manipulate single quantum objects. The Quantum Flagship is driving this revolution in Europe.

LEARN MORE

Maran van Heesch – maran.vanheesch@tno.nl