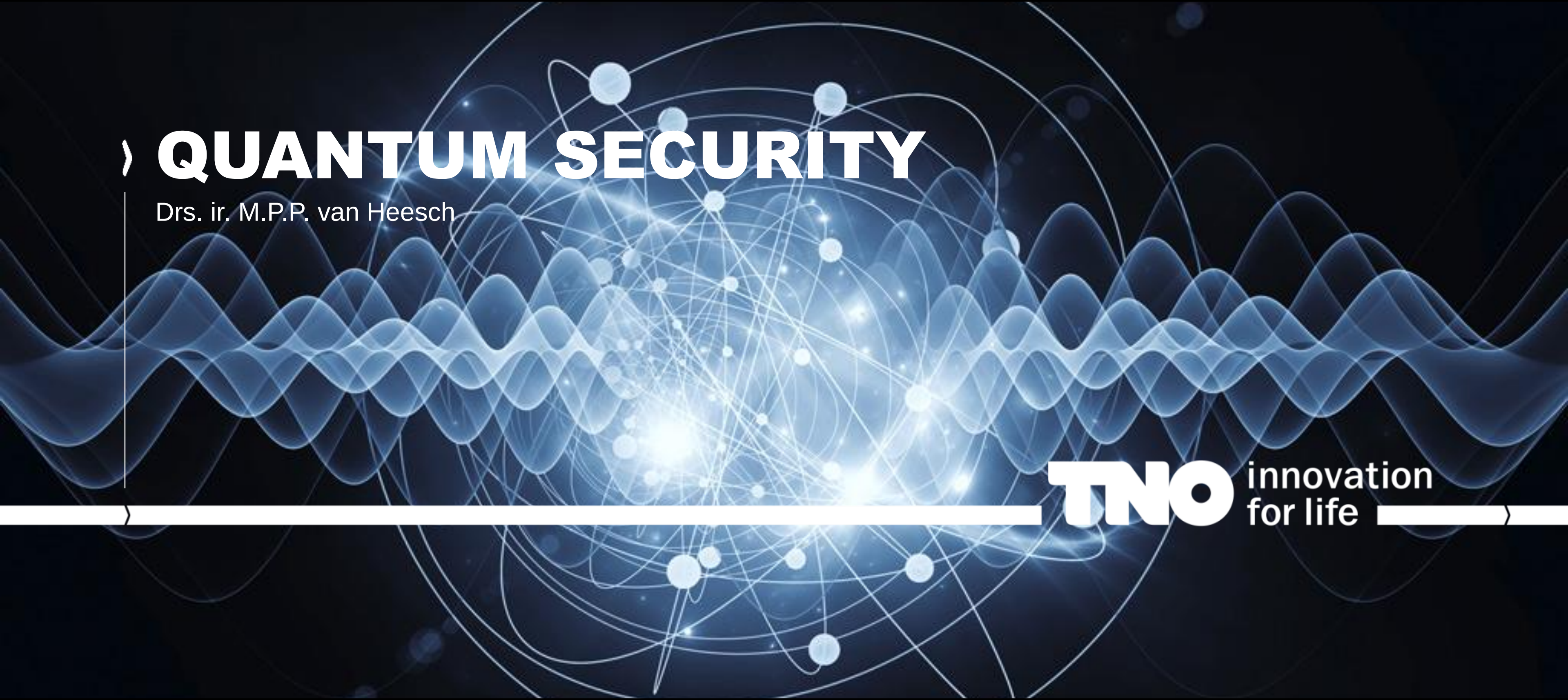
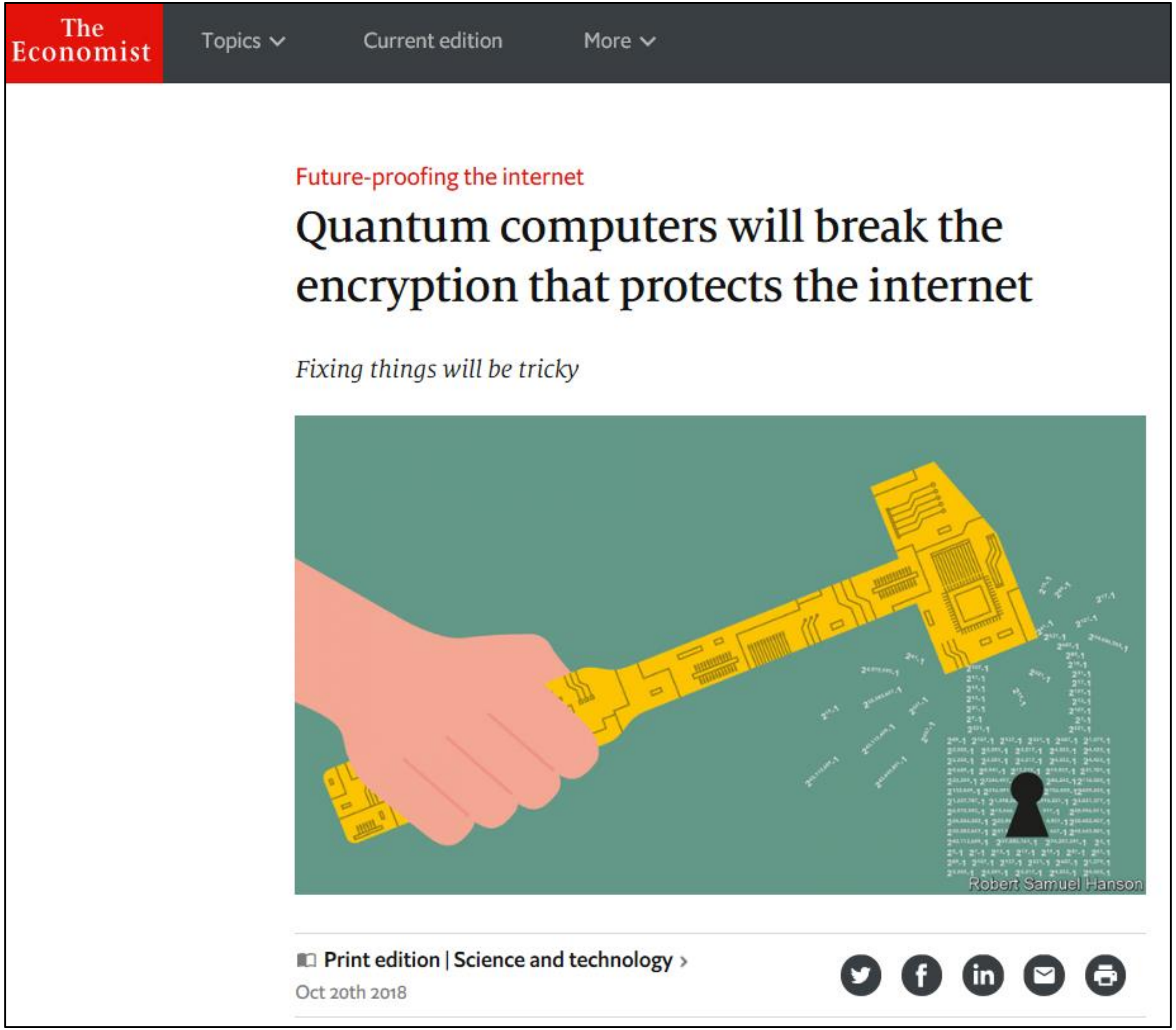
QUANTUM SECURITY

Drs. ir. M.P.P. van Heesch



TNO innovation for life



Future-proofing the internet

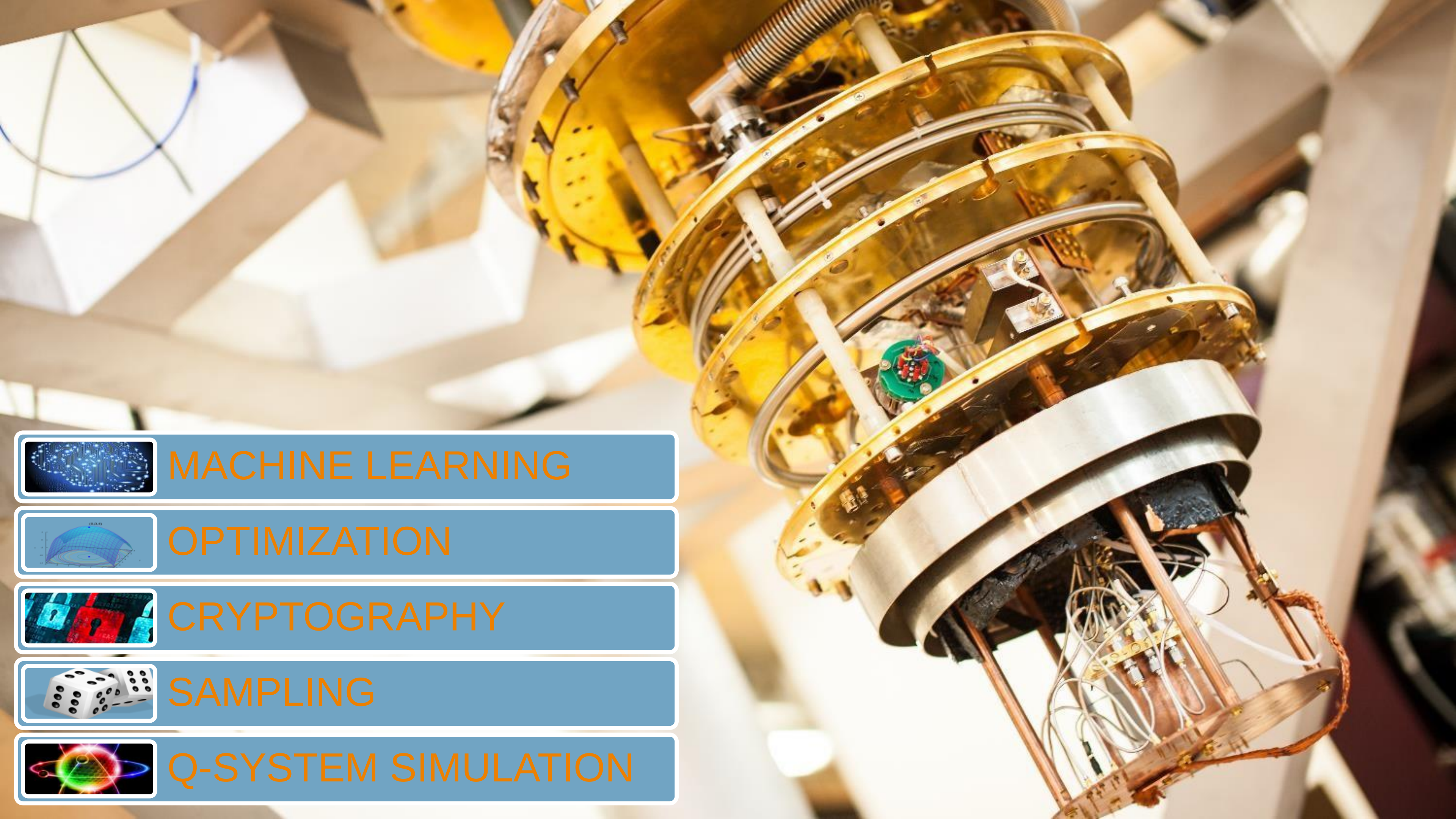
Quantum computers will break the encryption that protects the internet

Fixing things will be tricky

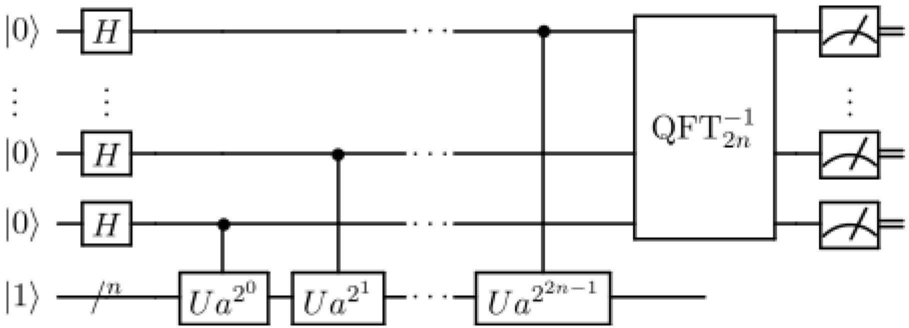
Robert Samuel Hanson

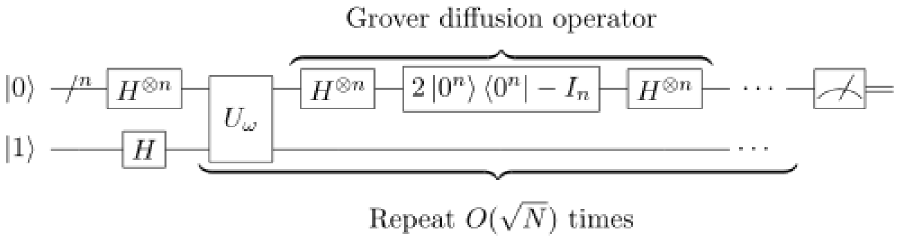
Print edition | Science and technology ›

Oct 20th 2018



- MACHINE LEARNING
- OPTIMIZATION
- CRYPTOGRAPHY
- SAMPLING
- Q-SYSTEM SIMULATION

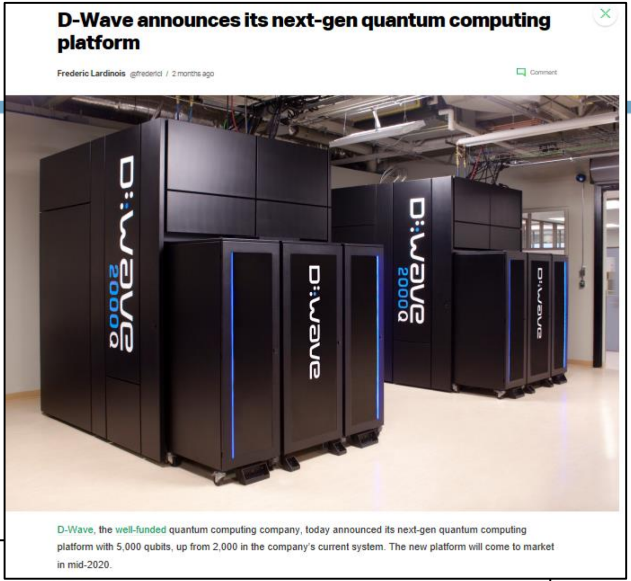



Grover diffusion operator
$|0\rangle$
n
$H^{\otimes n}$
$|1\rangle$
H
U_ω
$H^{\otimes n}$
$2|0^n\rangle\langle 0^n| - I_n$
$H^{\otimes n}$
Repeat $O(\sqrt{N})$ times

Broken:
RSA
ECC
DH

Weakend:
AES

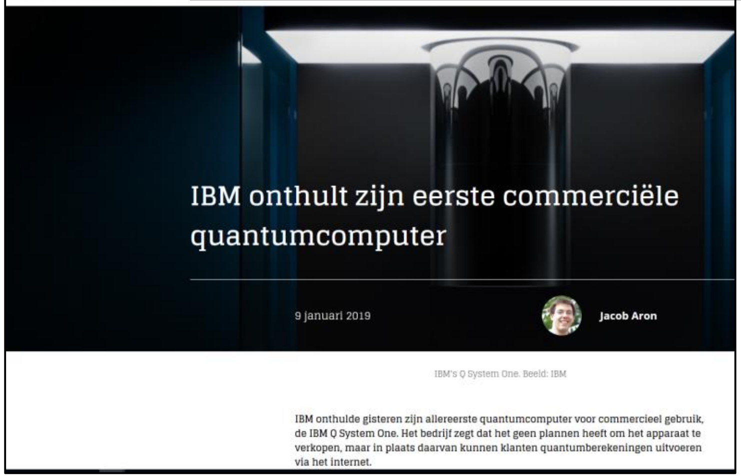
2000 qubits



D-Wave announces its next-gen quantum computing platform

Frederic Lardinois @fredericl / 2 months ago

D-Wave, the well-funded quantum computing company, today announced its next-gen quantum computing platform with 5,000 qubits, up from 2,000 in the company's current system. The new platform will come to market in mid-2020.



IBM onthult zijn eerste commerciële quantumcomputer

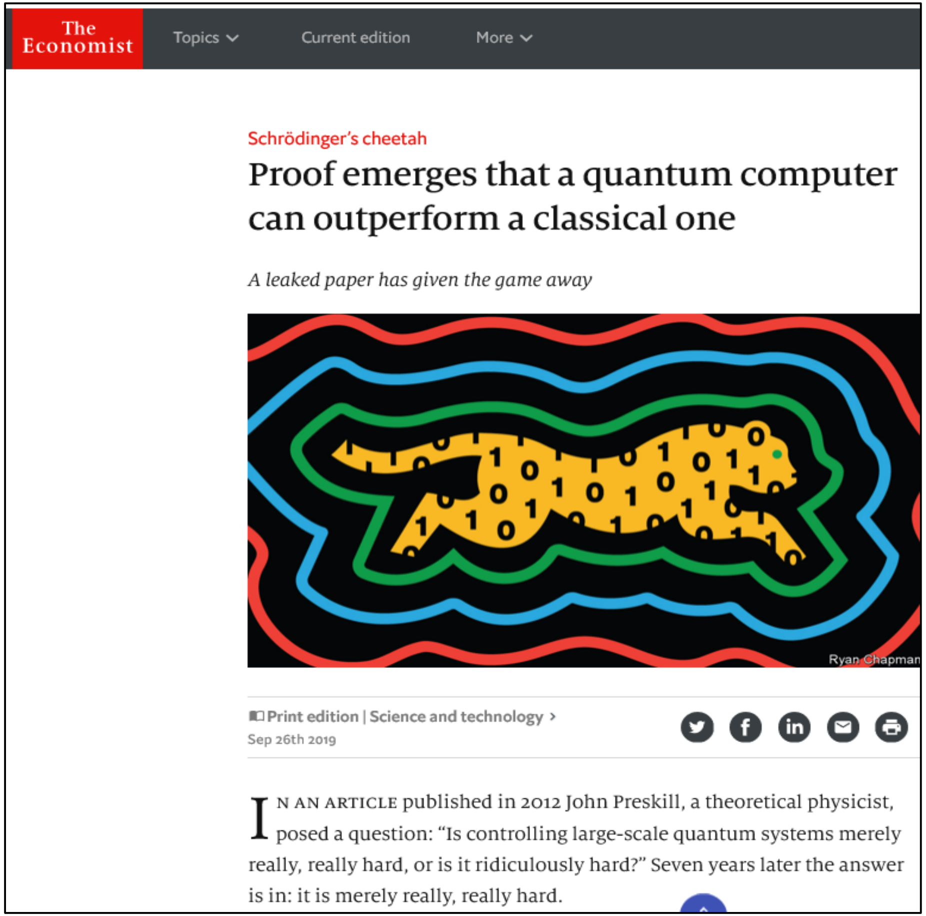
9 januari 2019

Jacob Aron

IBM's Q System One. Beeld: IBM

IBM onthulde gisteren zijn allereerste quantumcomputer voor commercieel gebruik, de IBM Q System One. Het bedrijf zegt dat het geen plannen heeft om het apparaat te verkopen, maar in plaats daarvan kunnen klanten quantumberekeningen uitvoeren via het internet.

53 qubits



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 ›

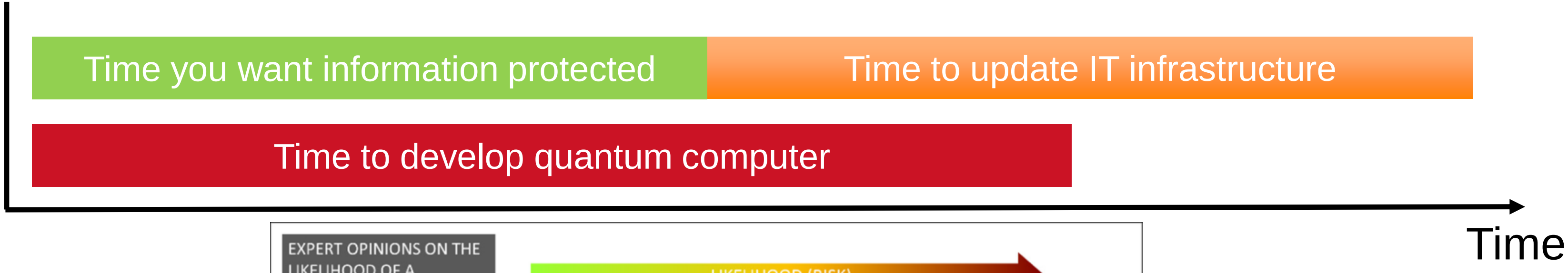
Sep 26th 2019

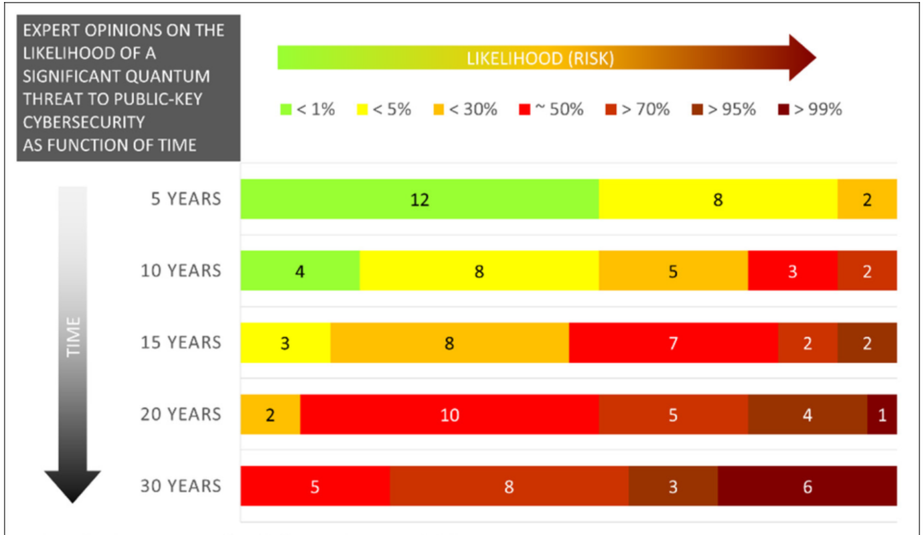
IN AN ARTICLE published in 2012 John Preskill, a theoretical physicist, posed a question: "Is controlling large-scale quantum systems merely really, really hard, or is it ridiculously hard?" Seven years later the answer is in: it is merely really, really hard.

Store now, decrypt later

https://commons.wikimedia.org/wiki/File:EFF_photograph_of_NSA%27s_Utah_Data_Center.jpg

WHY START NOW?


Time you want information protected
Time to update IT infrastructure
Time to develop quantum computer
Time



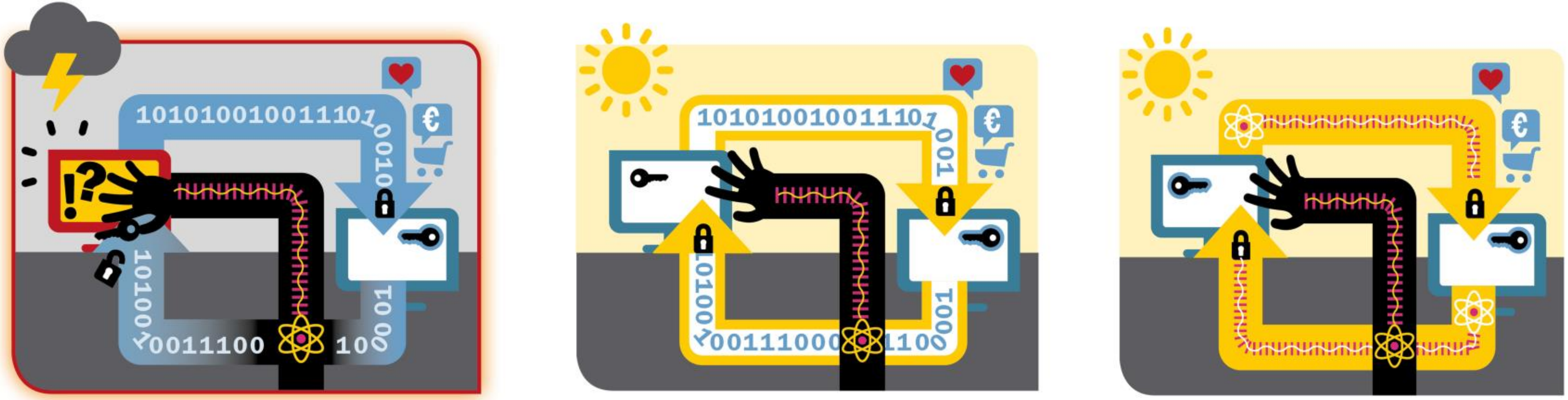
Numbers reflect how many experts (out of 22) assigned a certain probability range.

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

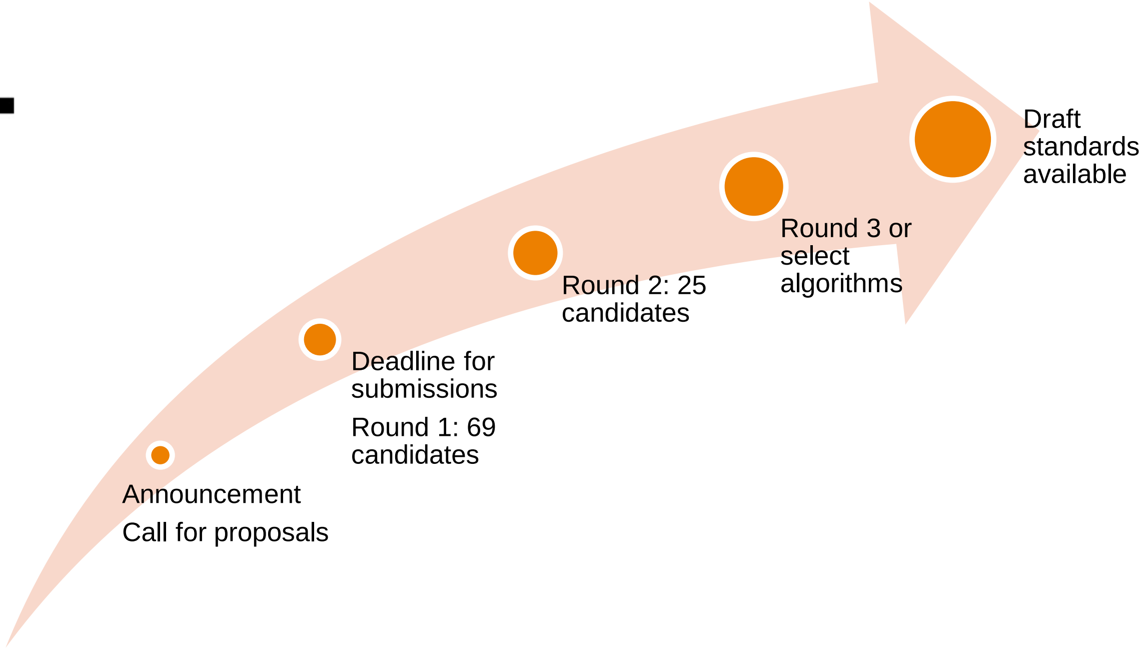
GETTING QUANTUM-READY

Broken:
RSA
ECC
DH

Weakend:
AES



STANDARDISATION: NIST



Announcement

Call for proposals

Deadline for submissions

Round 1: 69 candidates

Round 2: 25 candidates

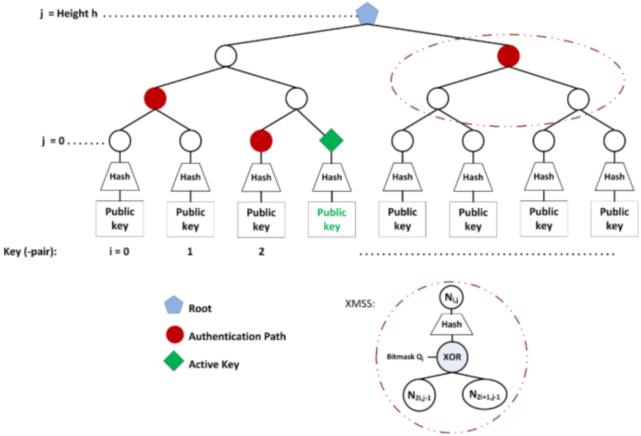
Round 3 or select algorithms

Draft standards available

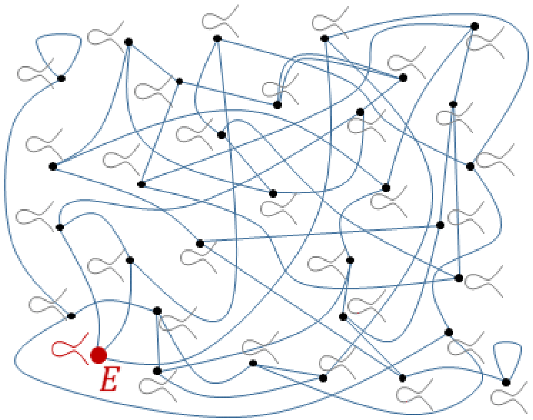
2016 2017 2019 2020/2021 ~2023

POST-QUANTUM CRYPTOGRAPHY

- Need to ***diversify*** the cryptographic protocols and associated mathematical problems.



Hash-based



Supersingular Isogenies

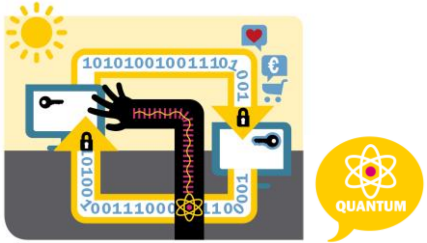


Figure: https://www.esat.kuleuven.be/cosic/elliptic-curves-are-quantum-dead-long-live-elliptic-curves/

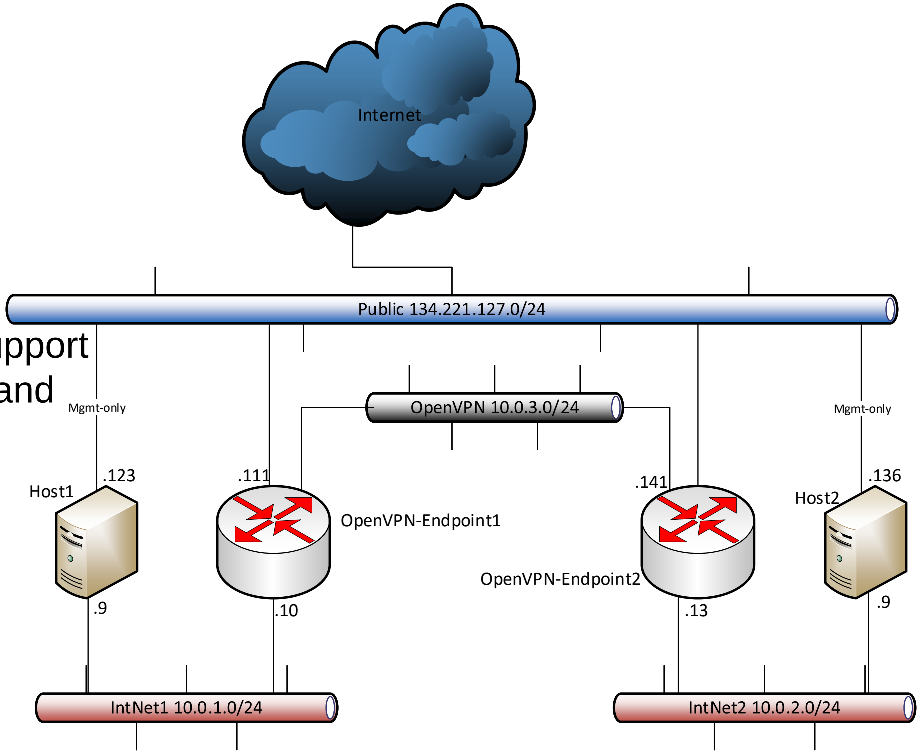
QUANTUM-SAFE VPN

- Prototype in Internal Cloud

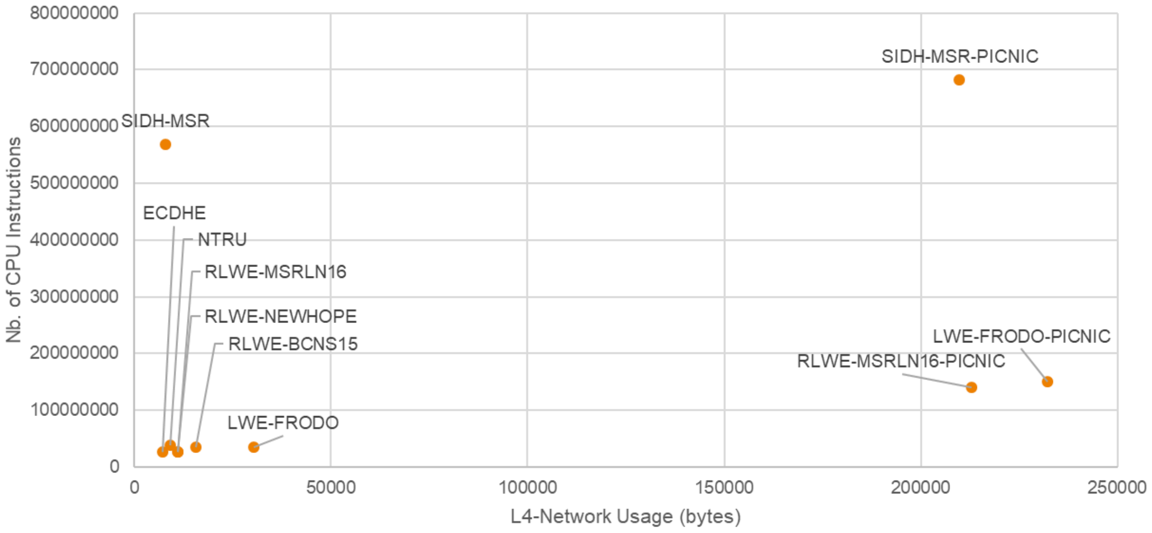
- Compiled OpenVPN with Post-Quantum Crypto support using shared objects from *OpenSSL-OQS*, *liboqs* and *lib_sigpicnic*

- Evaluated
  - Quantum-Safe Key Exchange
  - Quantum-Safe Hybrid Key Exchange (ECDHE+OQSKEX)
  - Quantum-Safe Authentication

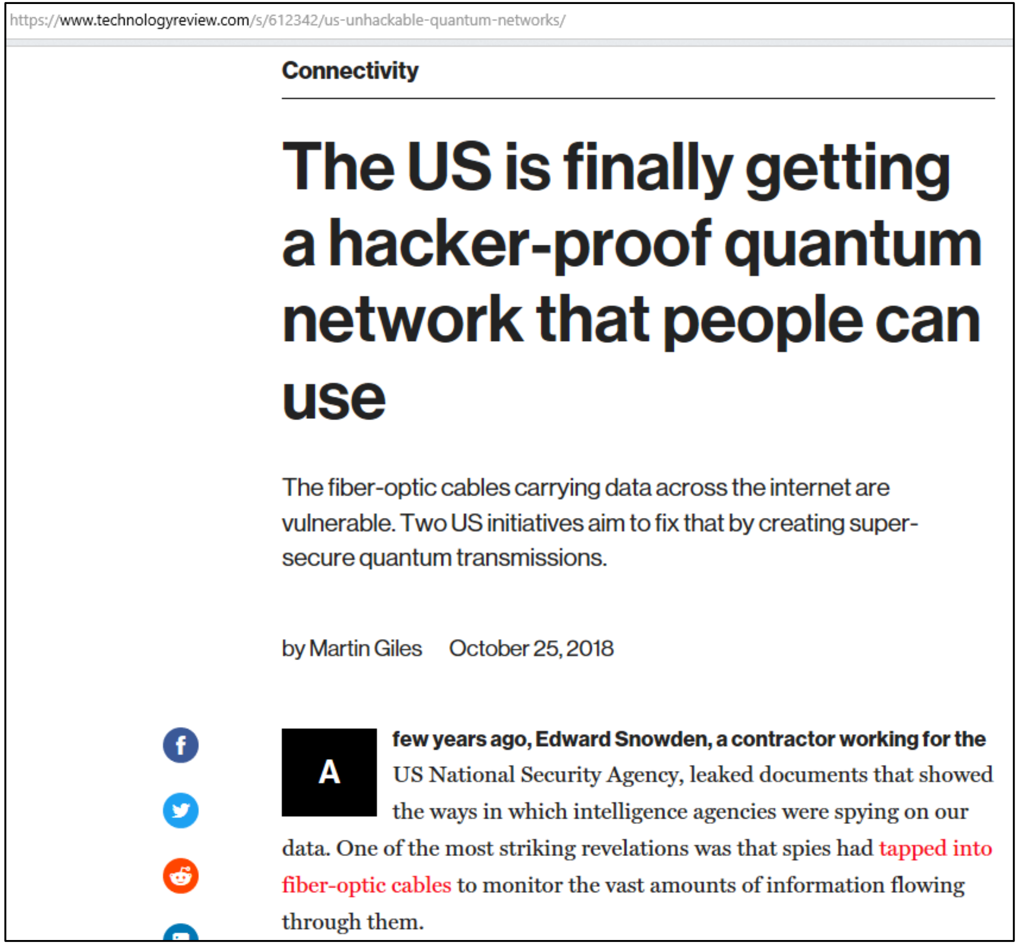
- Experiments using TLS 1.2 and TLS 1.3



QUANTUM-SAFE VPN (TLS 1.2) INCLUDING A SELF-SIGNING CA



Towards Quantum-Safe VPNs and Internet https://eprint.iacr.org/2019/1277



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

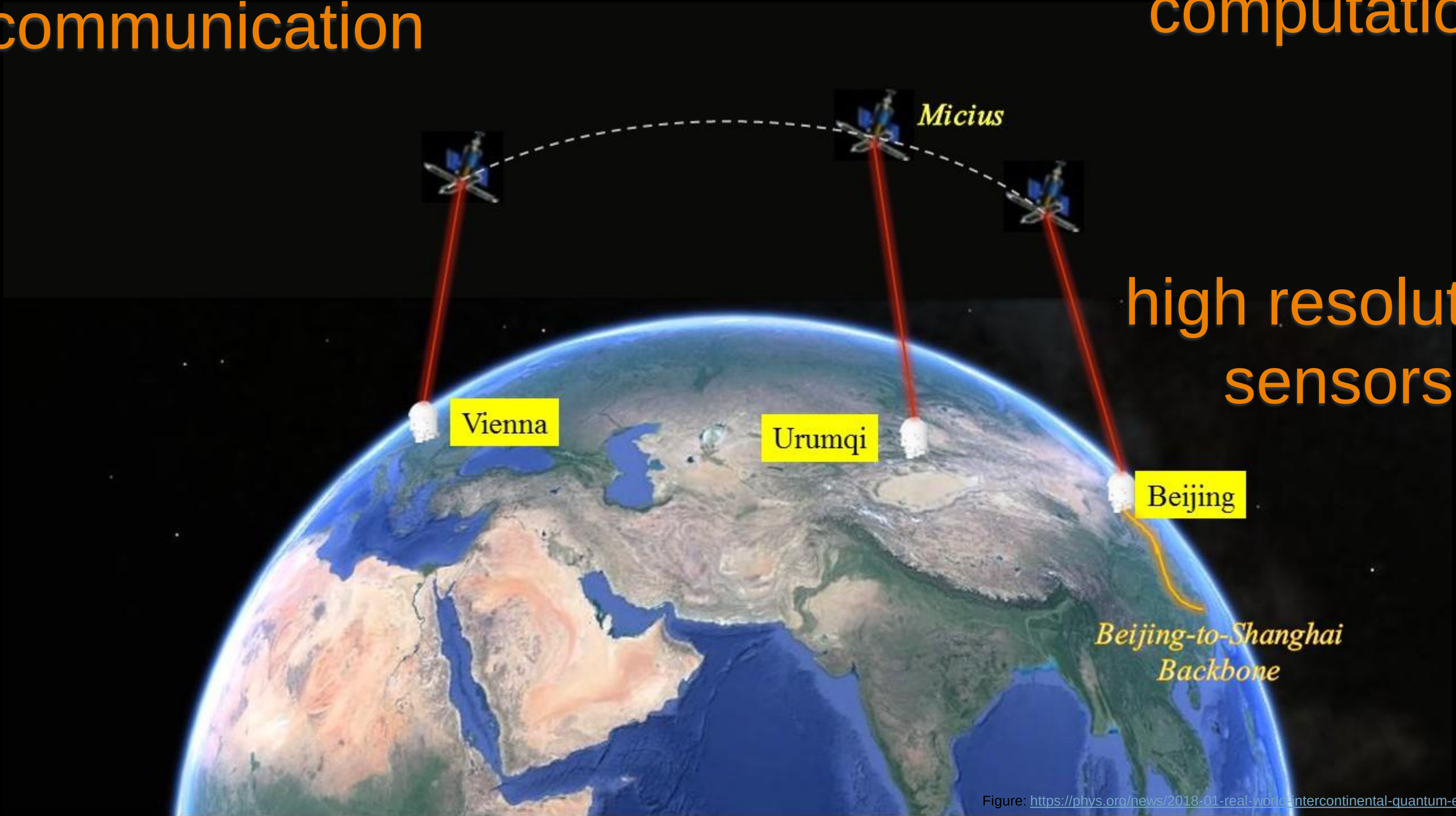
The fiber-optic cables carrying data across the internet are vulnerable. Two US initiatives aim to fix that by creating super-secure quantum transmissions.

by Martin Giles October 25, 2018

A few years ago, Edward Snowden, a contractor working for the US National Security Agency, leaked documents that showed the ways in which intelligence agencies were spying on our data. One of the most striking revelations was that spies had tapped into fiber-optic cables to monitor the vast amounts of information flowing through them.

secure communication

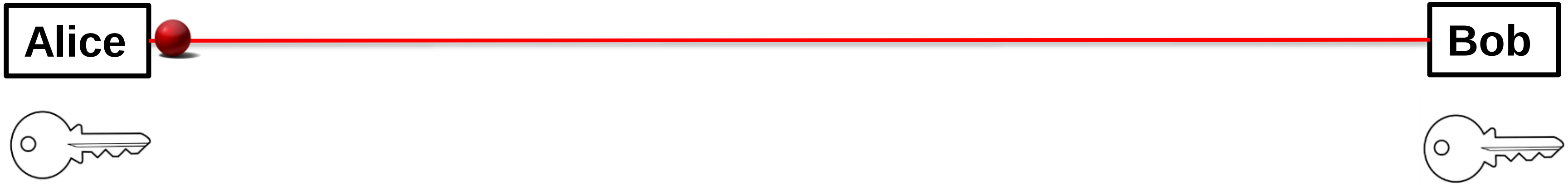
distributed computation



high resolution sensors

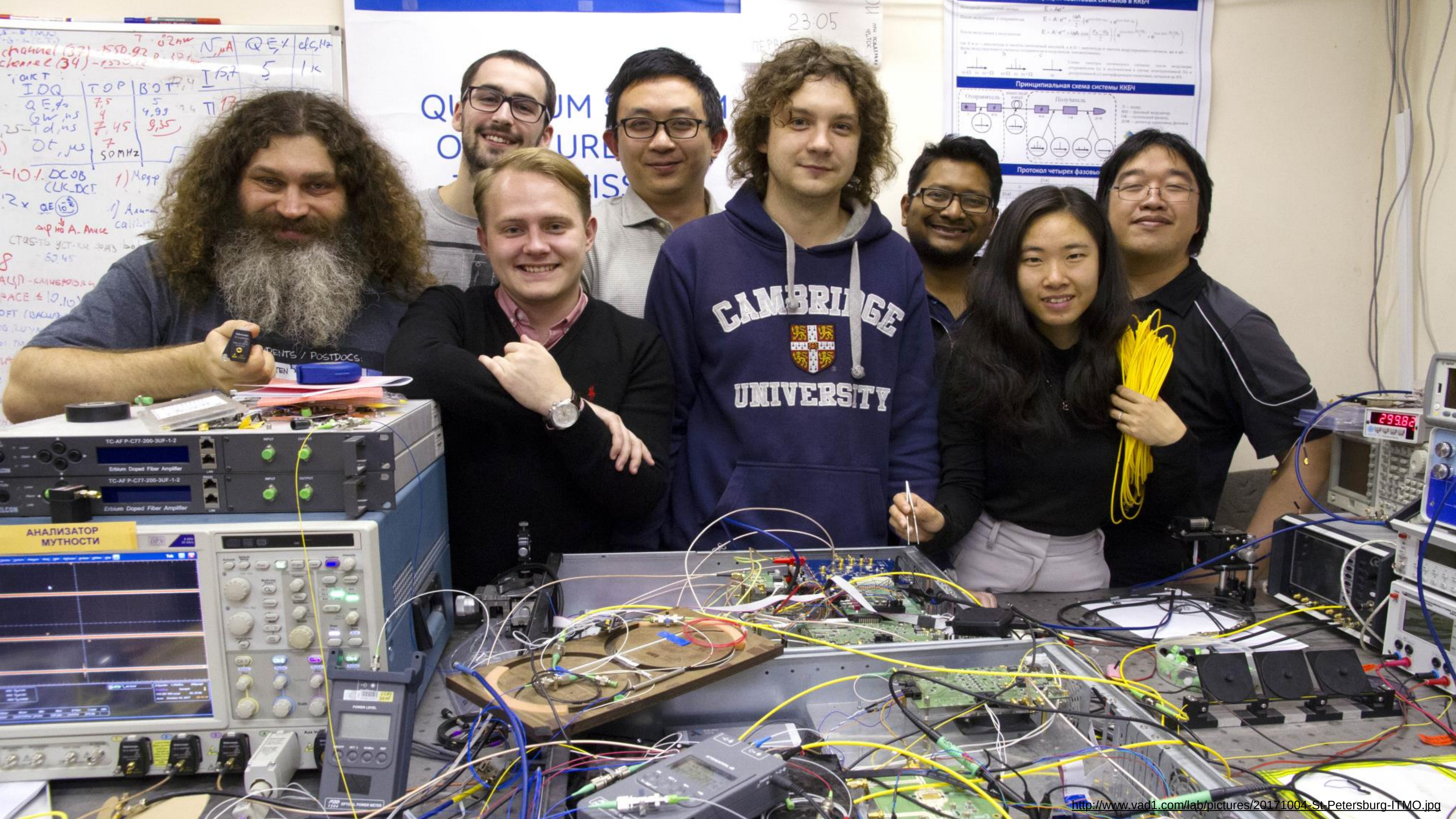
Figure: https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html

QUANTUM KEY DISTRIBUTION (QKD)

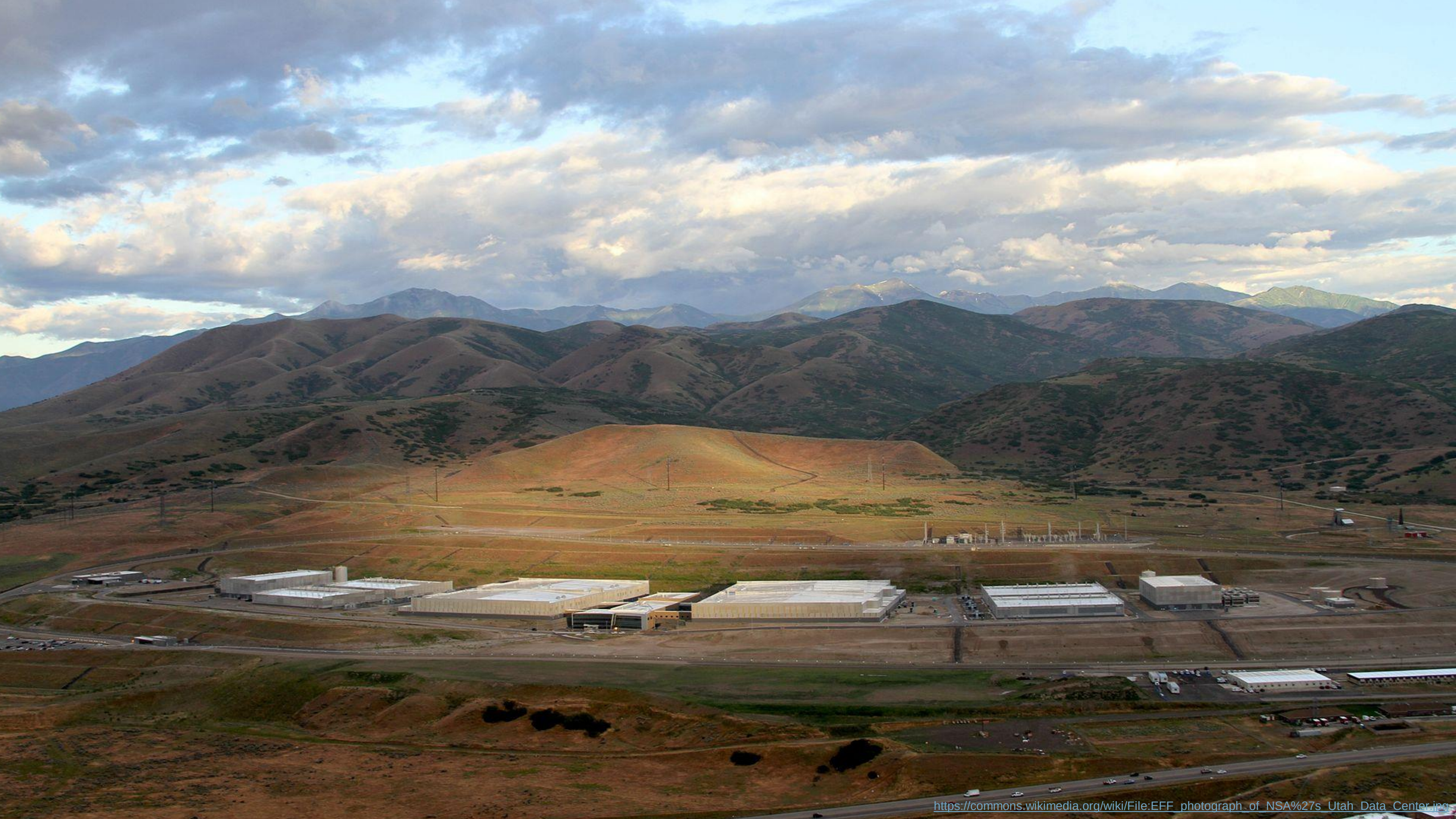


- Promise: Inherent security

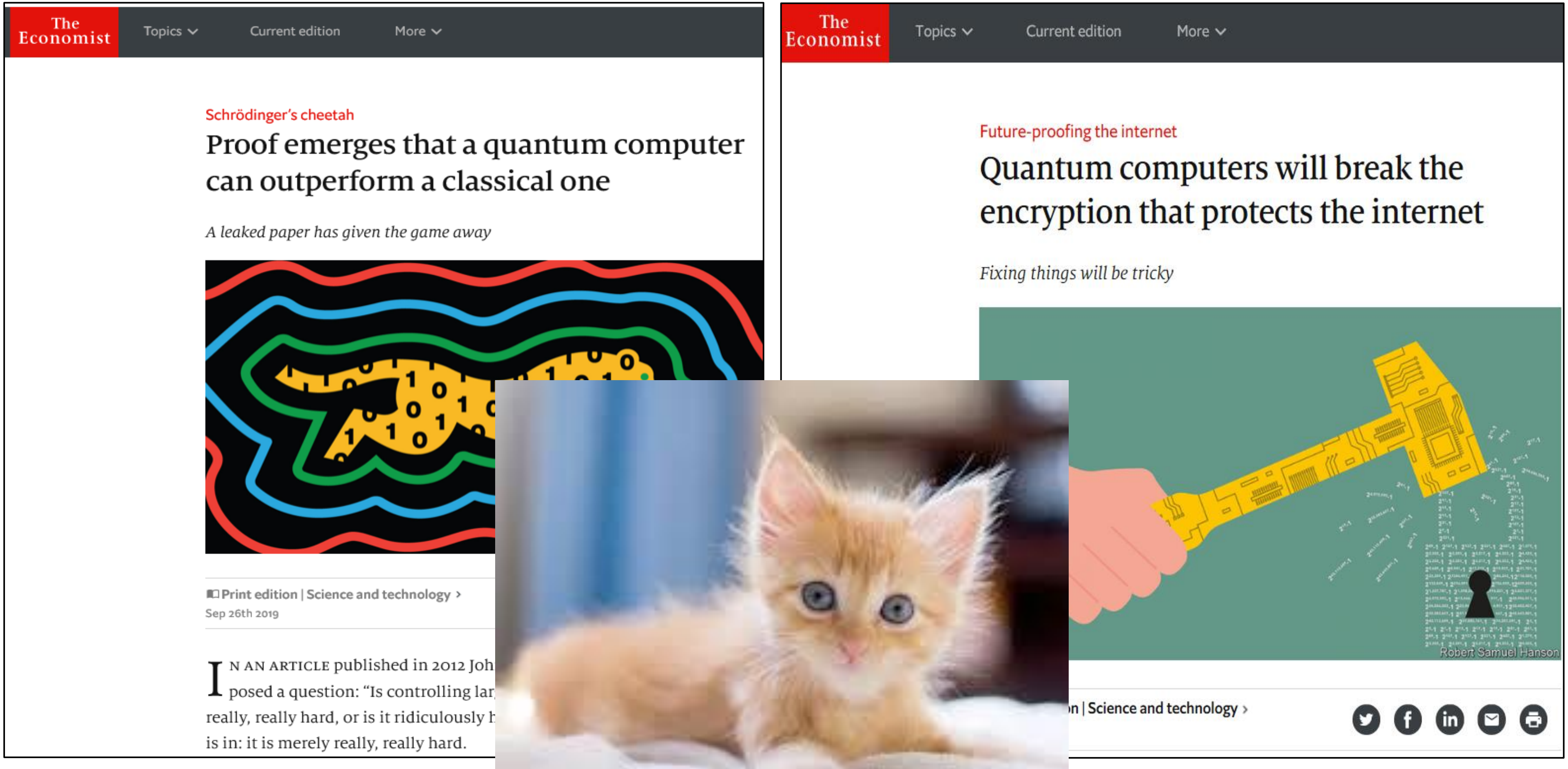
Attack	Target component	Tested system
Distinguishability of decoy states A. Huang *et al.*, Phys. Rev. A **98**, 012330 (2018)	laser in Alice	3 research systems
Intersymbol interference K. Yoshino *et al.*, poster at QCrypt (2016)	intensity modulator in Alice	research system
Laser damage V. Makarov *et al.*, Phys. Rev. A **94**, 030302 (2016); A. Huang *et al.*, poster at QCrypt (2018)	any	5 commercial & 1 research systems
Spatial efficiency mismatch M. Rau *et al.*, IEEE J. Sel. Top. Quantum Electron. **21**, 6600905 (2015); S. Sajeed *et al.*, Phys. Rev. A **91**, 062301 (2015)	receiver optics	2 research systems
Pulse energy calibration S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)	classical watchdog detector	ID Quantique
Trojan-horse I. Khan *et al.*, presentation at QCrypt (2014)	phase modulator in Alice	SeQureNet
Trojan-horse N. Jain *et al.*, New J. Phys. **16**, 123030 (2014); S. Sajeed *et al.*, Sci. Rep. **7**, 8403 (2017)	phase modulator in Bob	ID Quantique
Detector saturation H. Qin, R. Kumar, R. Alleaume, Proc. SPIE 88990N (2013)	homodyne detector	SeQureNet
Shot-noise calibration P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A **87**, 062313 (2013)	classical sync detector	SeQureNet
Wavelength-selected PNS M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A **86**, 032310 (2012)	intensity modulator	(theory)
Multi-wavelength H.-W. Li *et al.*, Phys. Rev. A **84**, 062308 (2011)	beamsplitter	research system
Deadtime H. Weier *et al.*, New J. Phys. **13**, 073024 (2011)	single-photon detector	research system
Channel calibration N. Jain *et al.*, Phys. Rev. Lett. **107**, 110501 (2011)	single-photon detector	ID Quantique
Faraday-mirror S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A **83**, 062331 (2011)	Faraday mirror	(theory)
Detector control I. Gerhardt *et al.*, Nat. Commun. **2**, 349 (2011); L. Lydersen *et al.*, Nat. Photonics **4**, 686 (2010)	single-photon detector	ID Quantique, MagiQ, research systems



http://www.vad1.com/lab/pictures/20171004-St-Petersburg-ITMO.jpg



https://commons.wikimedia.org/wiki/File:EFF_photograph_of_NSA%27s_Utah_Data_Center.jpg



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

Print edition | Science and technology ›

Sep 26th 2019

IN AN ARTICLE published in 2012 Joh
posed a question: "Is controlling lar
really, really hard, or is it ridiculously h
is in: it is merely really, really hard.

The Economist

Topics ⌄ Current edition More ⌄

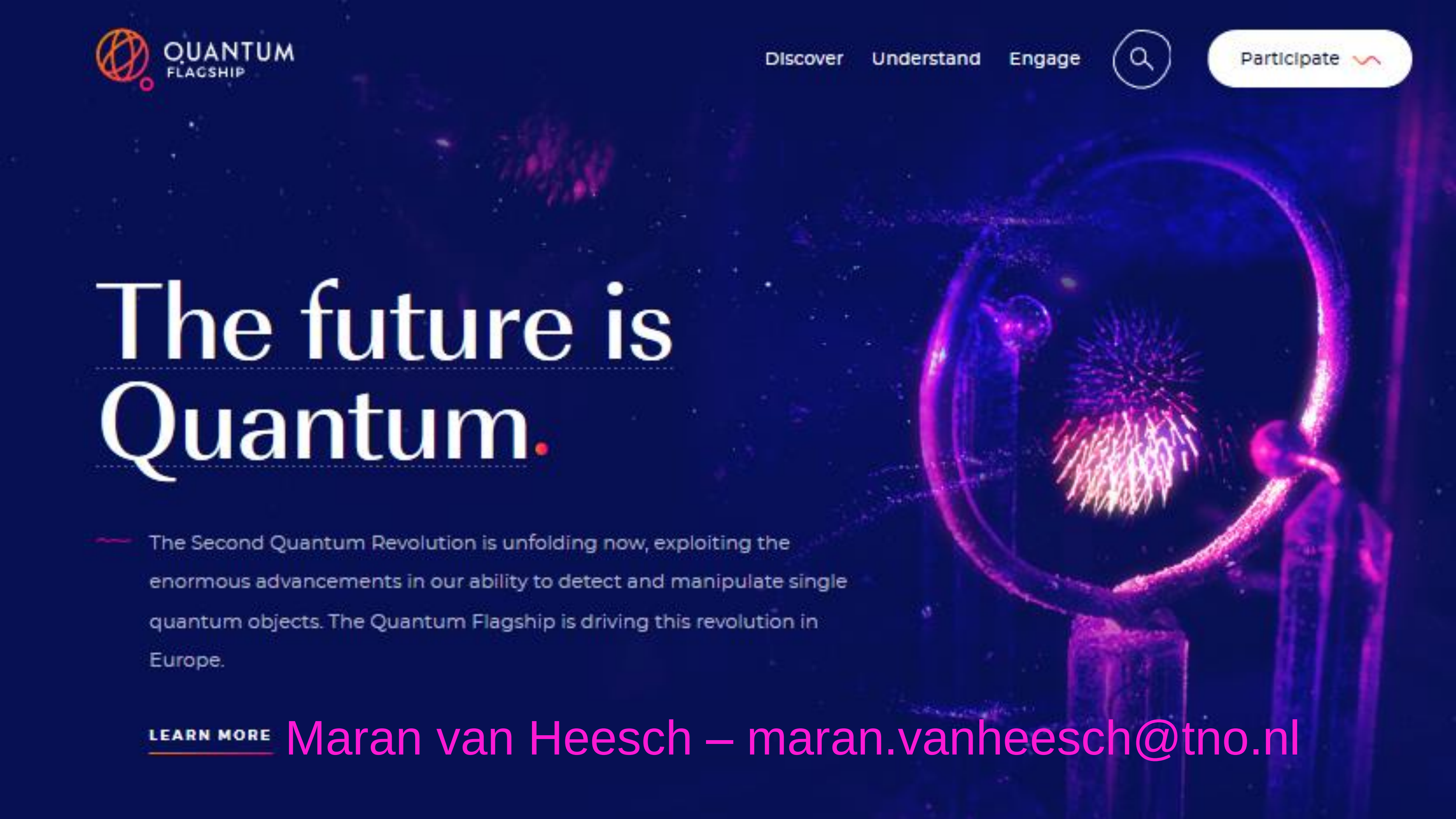
Future-proofing the internet

Quantum computers will break the encryption that protects the internet

Fixing things will be tricky

Robert Samuel Hanson

n | Science and technology ›



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.

Maran van Heesch – maran.vanheesch@tno.nl