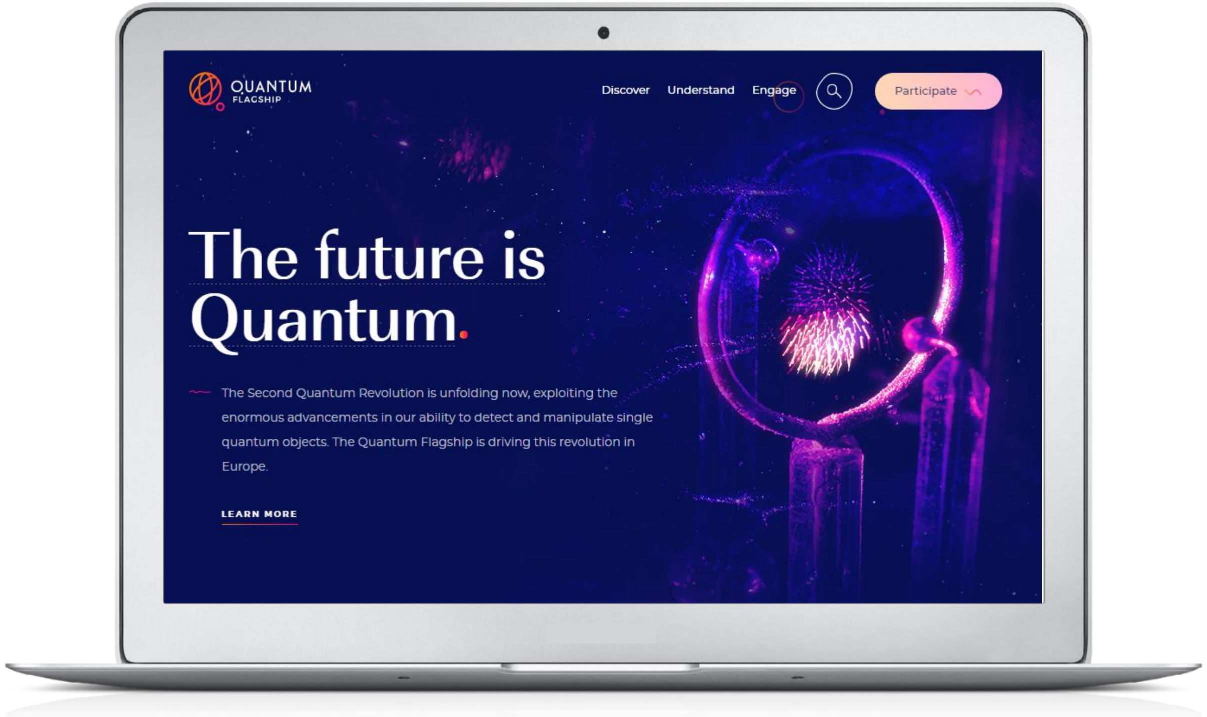
Secure Strategies for Past, Present & Future Communications

EPIC Quantum Technology Meeting

Bruno Huttner – ID Quantique

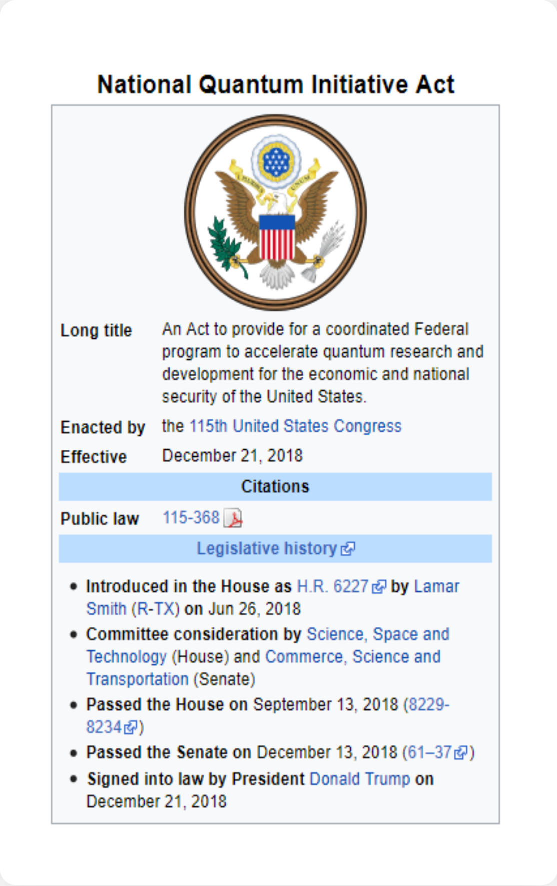
09/04/2021

Quantum has become a major government focus in EU, USA, & Asia



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.



National Quantum Initiative Act

Long title	An Act to provide for a coordinated Federal program to accelerate quantum research and development for the economic and national security of the United States.
Enacted by	the 115th United States Congress
Effective	December 21, 2018
Citations	
Public law	115-368
Legislative history	

- **Introduced in the House as** H.R. 6227 **by** Lamar Smith (R-TX) **on** Jun 26, 2018
- **Committee consideration by** Science, Space and Technology (House) and Commerce, Science and Transportation (Senate)
- **Passed the House on** September 13, 2018 (8229-8234)
- **Passed the Senate on** December 13, 2018 (61–37)
- **Signed into law by President** Donald Trump **on** December 21, 2018

But there are always two sides of a story…

THE QUANTUM COMPUTER

Opportunities

- New Materials and Chemicals
- Optimizing designs
- Allocation or resources
- Machine Learning

Dr. Jekyll

Mr. Hyde

Threats

- Cybersecurity infrastructure

When do we need to worry?

Today

Q-day

Before

Confidential information

After

All the cybersecurity infrastructure

Protect confidential information NOW!

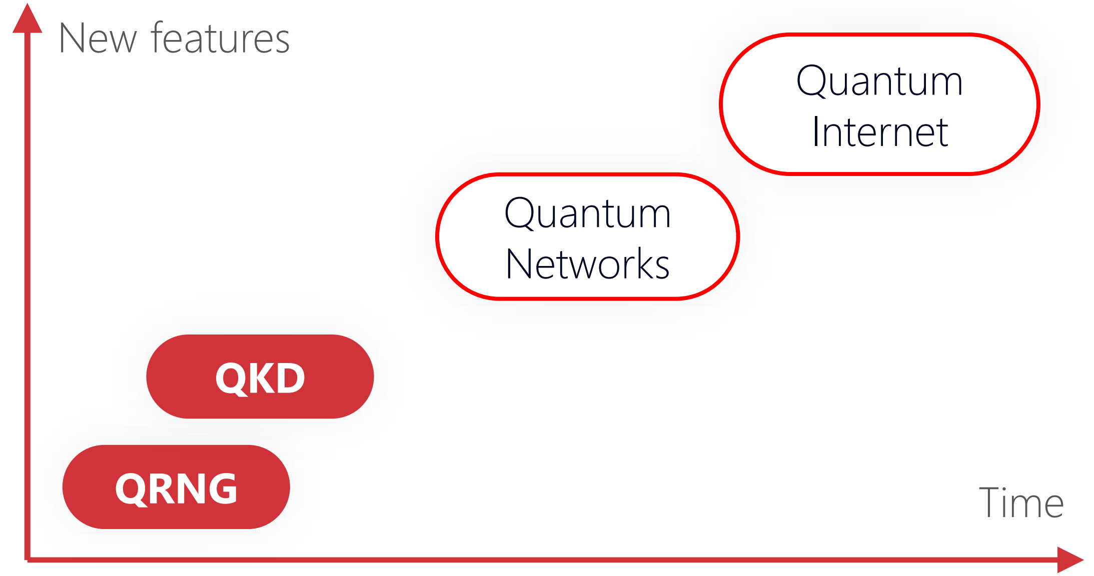
How to address the quantum threats? Quantum-Safe Solutions

Classical solutions

- Post-Quantum Cryptography (PQC).
- Find classical algorithms to replace current ones
- Choose mathematical problems known/believed to be resistant to the Quantum Computer
- The NIST process is exactly doing this now…

Quantum vs. Quantum

Use quantum systems and properties against the Quantum Computer

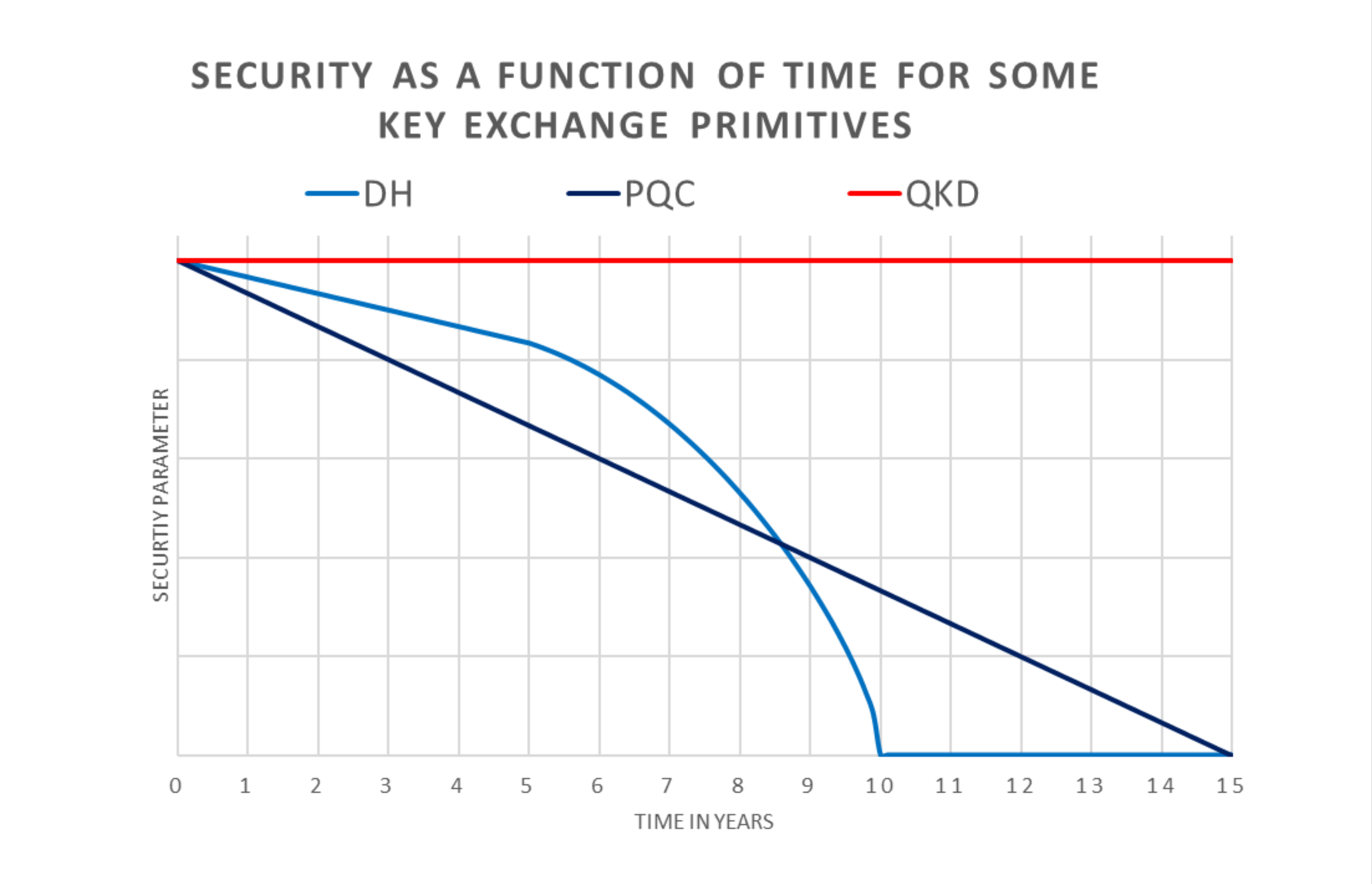


Classical & Quantum solutions: we need both!

Different solutions for different needs…

Crypto function	Solution
Randomness – Entropy generation	Quantum (QRNG)
Authentication – Signature	Maths (PQC) & Physical (PUF…)
Key Exchange Mechanism	Maths (PQC) & Quantum (QKD)
Encryption	Maths

QKD vs. PQC: Time-dependence is the essence!

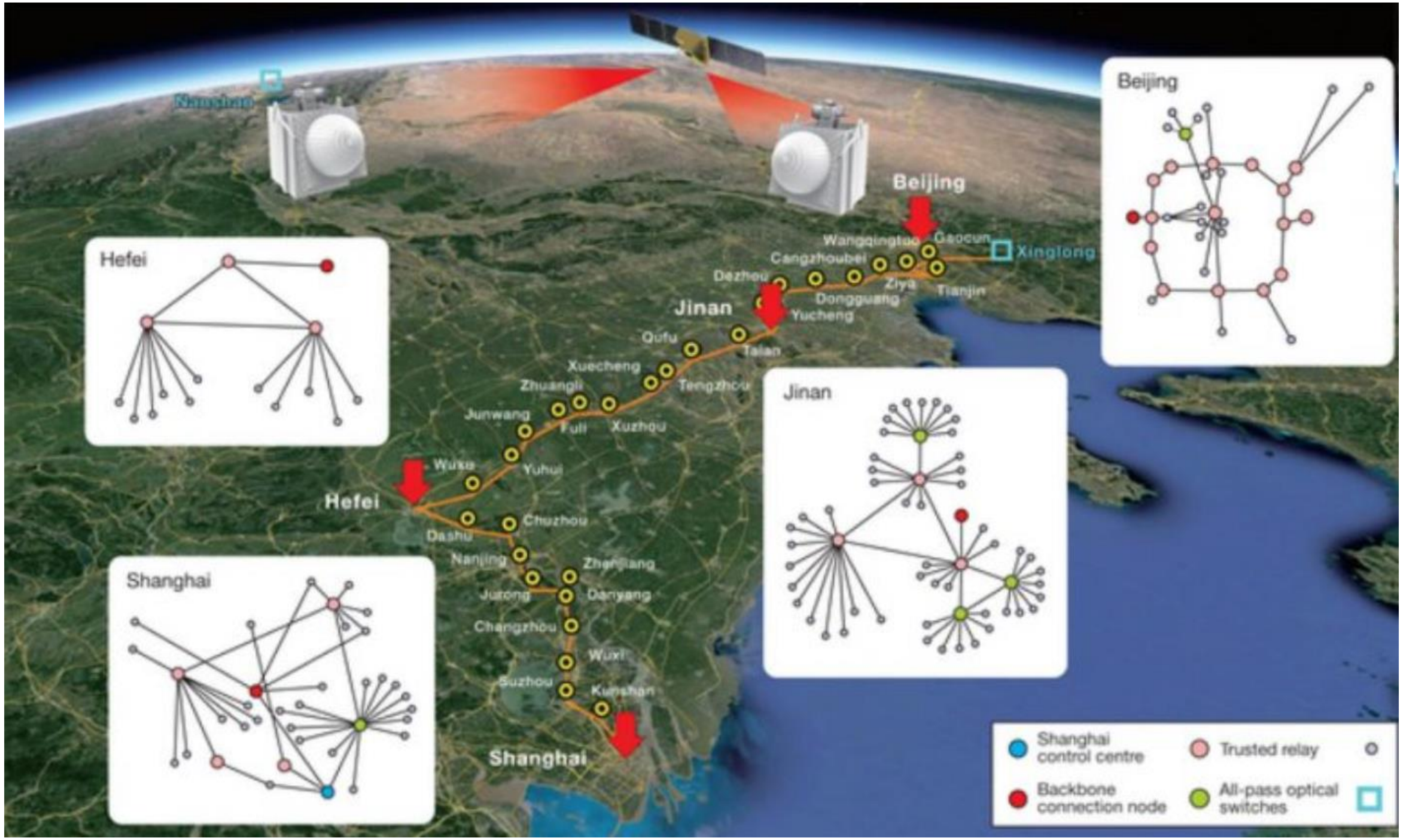


- All computational security comes with an expiry date

- Integrate QKD as Key Exchange Mechanism for high-valued information with long-term confidentiality requirements

- Adds one extra layer of security

Today: The Chinese integrated quantum network based on trusted nodes



Tomorrow: a worldwide Quantum Communication infrastructure

- Build a quantum infrastructure
- a.k.a: **The Quantum Internet**
- Each node stores and exchanges qubits with the others

ID Quantique

Quantum.
Trust enabled for the future

Q & A

bruno.huttner@idquantique.com | www.idquantique.com

ID Quantique

Founded in 2001

3 Product lines:

1. Quantum Random Number Generation
2. Quantum-Safe Security
3. Quantum Sensing

High-quality engineering

Best-in-class performance

Trust

Operational simplicity