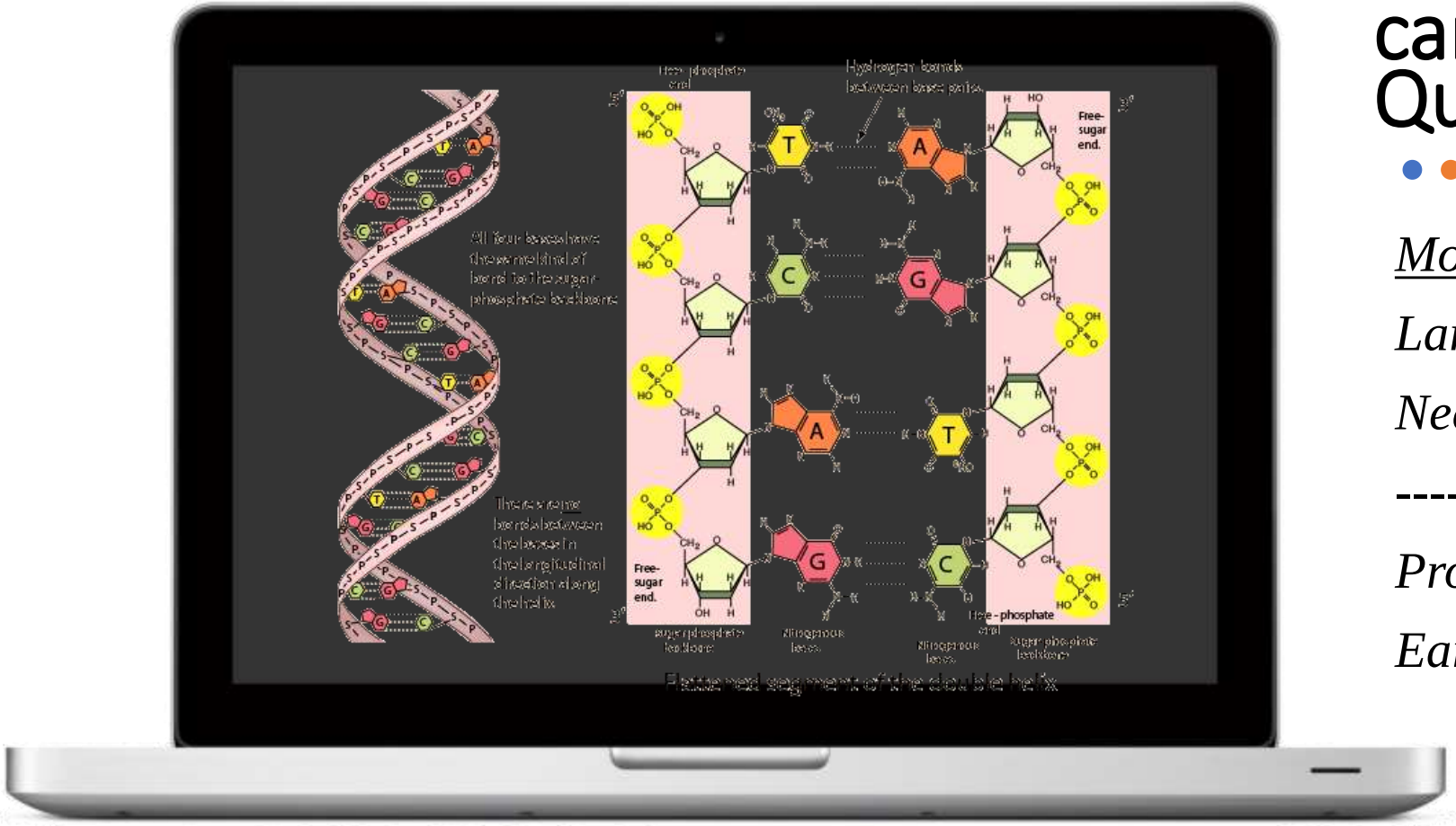
Our Secure Quantum Future

Cybersecurity in the era of Quantum Computing

Jaya Baloo. **@ jayabaloo**

CISO AVAST



What type of problems can we solve with a Quantum Computer

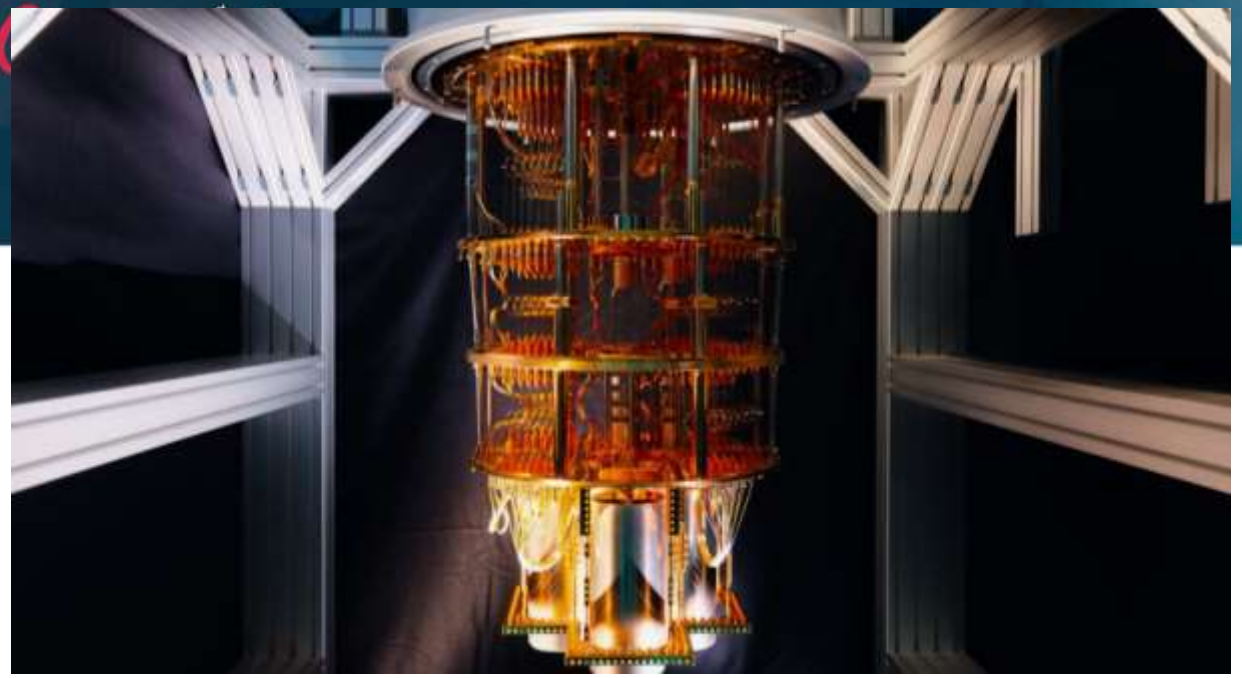
<u>Moore Vs. Amdahl</u>

Large data set problems

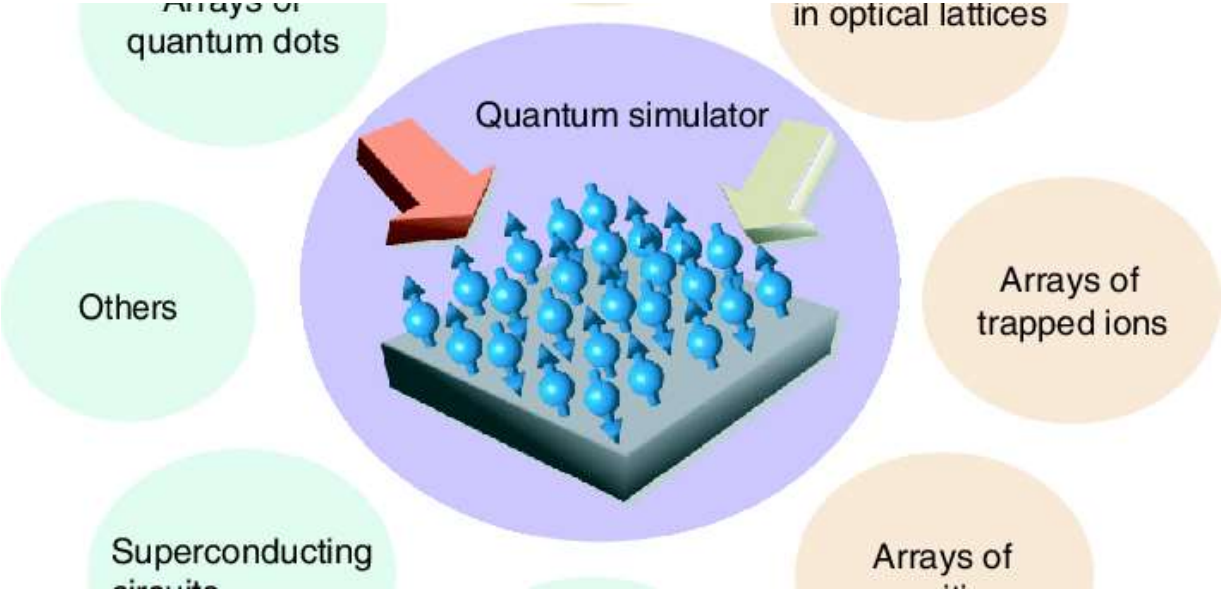
Needle in haystack problems

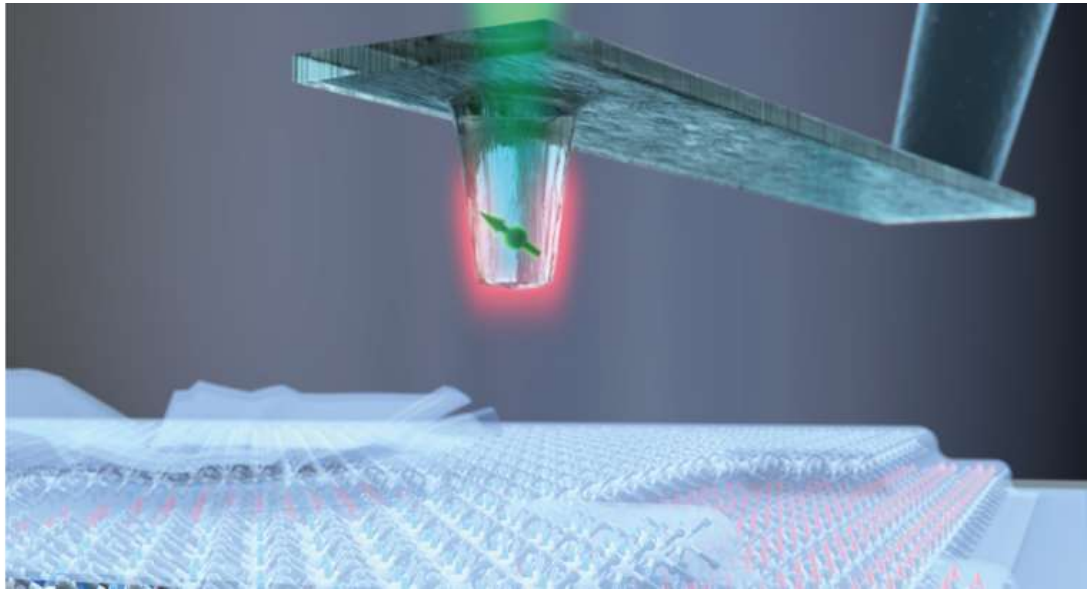
Protein mapping and drug interaction

Earlier detection of cancer

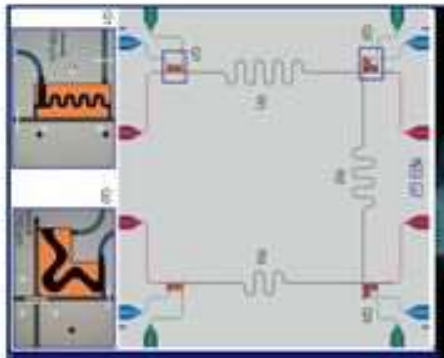
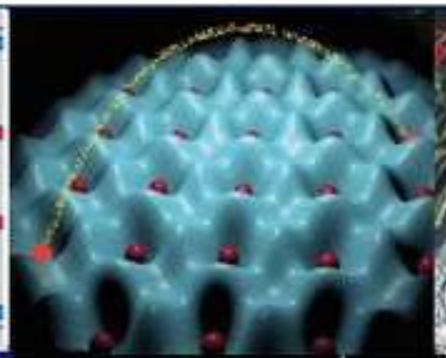
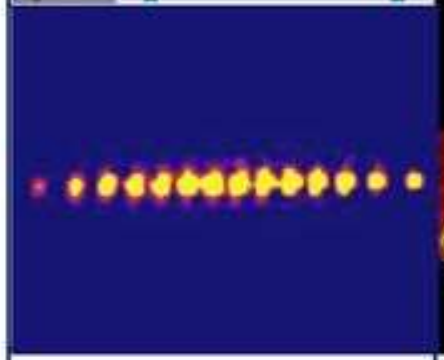
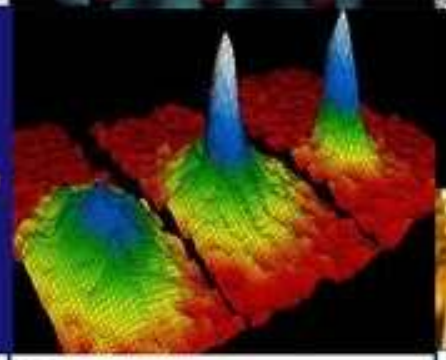
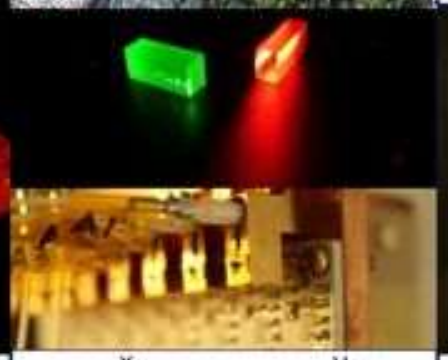
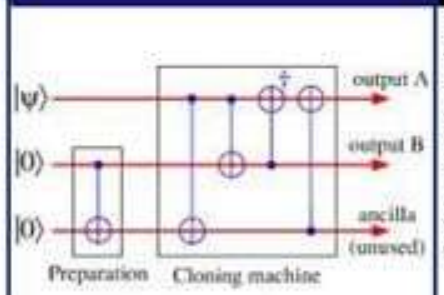
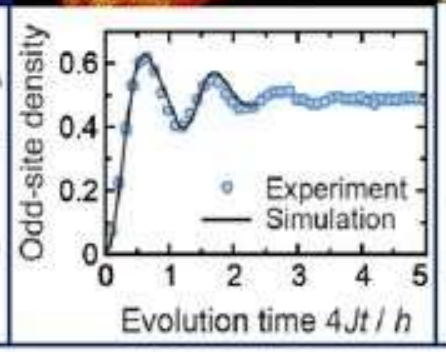
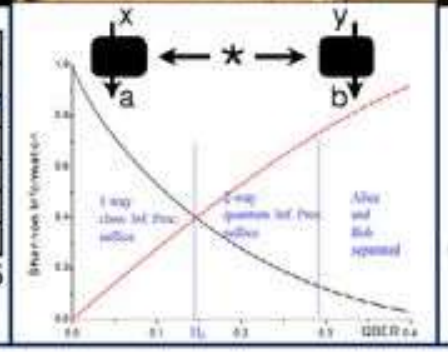



The Quantum Internet
Fault-tolerant quantum memories are used to build repeaters and switches for high-fidelity high-rate quantum communications over 1000s of km
Secure Communications
Quantum Multi-User Applications
Sensing,Timing, GPS
Networked Quantum Computing
QUANTUM REPEATER (QR)
QUANTUM SWITCH (QS)
QUANTUM COMPUTER (QC)
USER


quantum dots
in optical lattices
Quantum simulator
Others
Arrays of trapped ions
Superconducting
Arrays of



Quantum Technologies Flagship

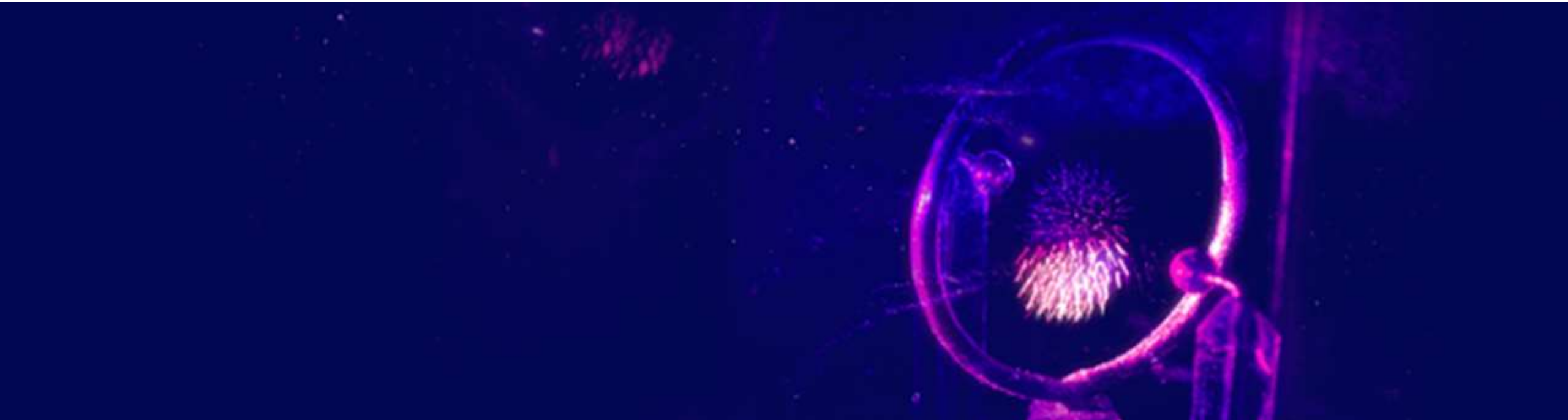
	Quantum Computers: Hardware & Software	Quantum Simulators	Quantum Communication: Devices & Systems	Quantum Sensing & Metrology
Quantum Engineering & Control				
Enabling Science				
Theory, Algorithms & Protocols				$\|\Psi\rangle \propto \|N,0\rangle - \|0,N\rangle$ $\mathrm{QFI} = 4\,\mathrm{var}_\psi(H)$

QUANTUM FLAGSHIP VISION

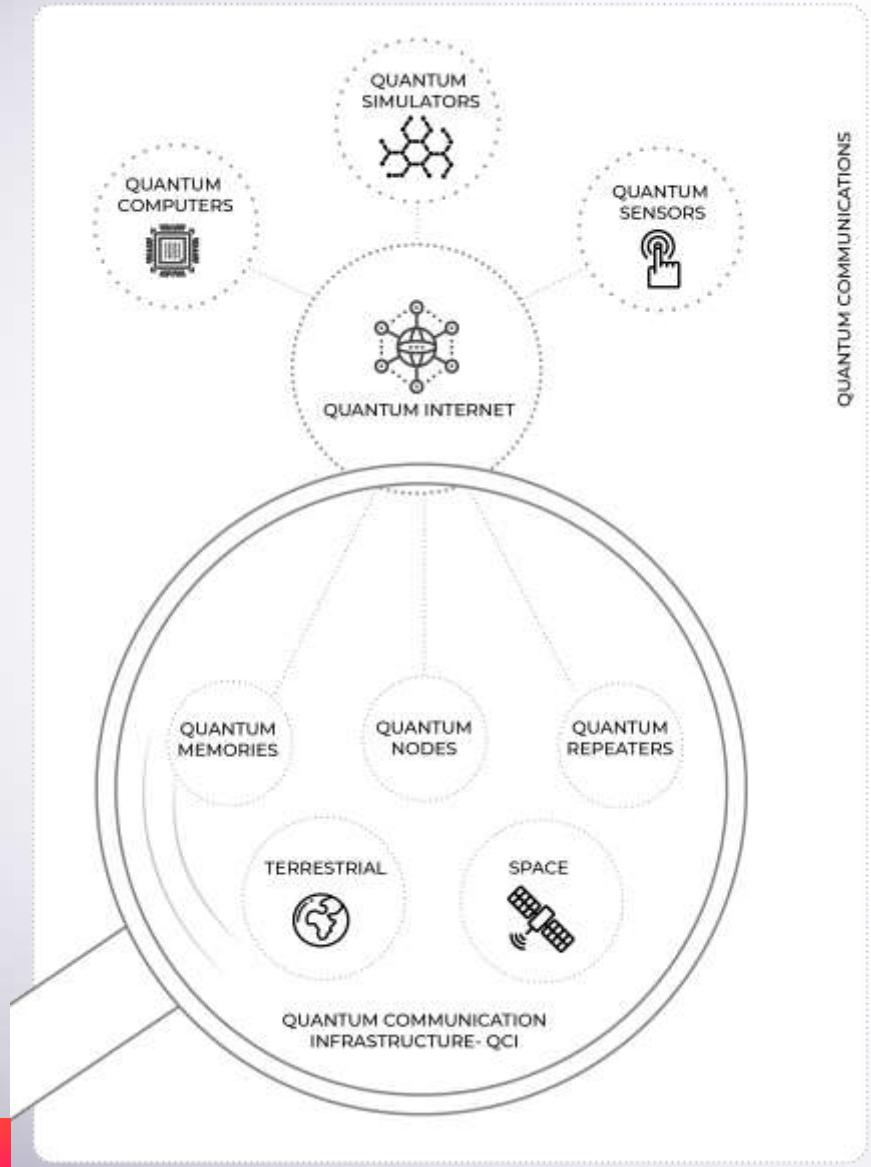
Consolidate and expand global scientific leadership

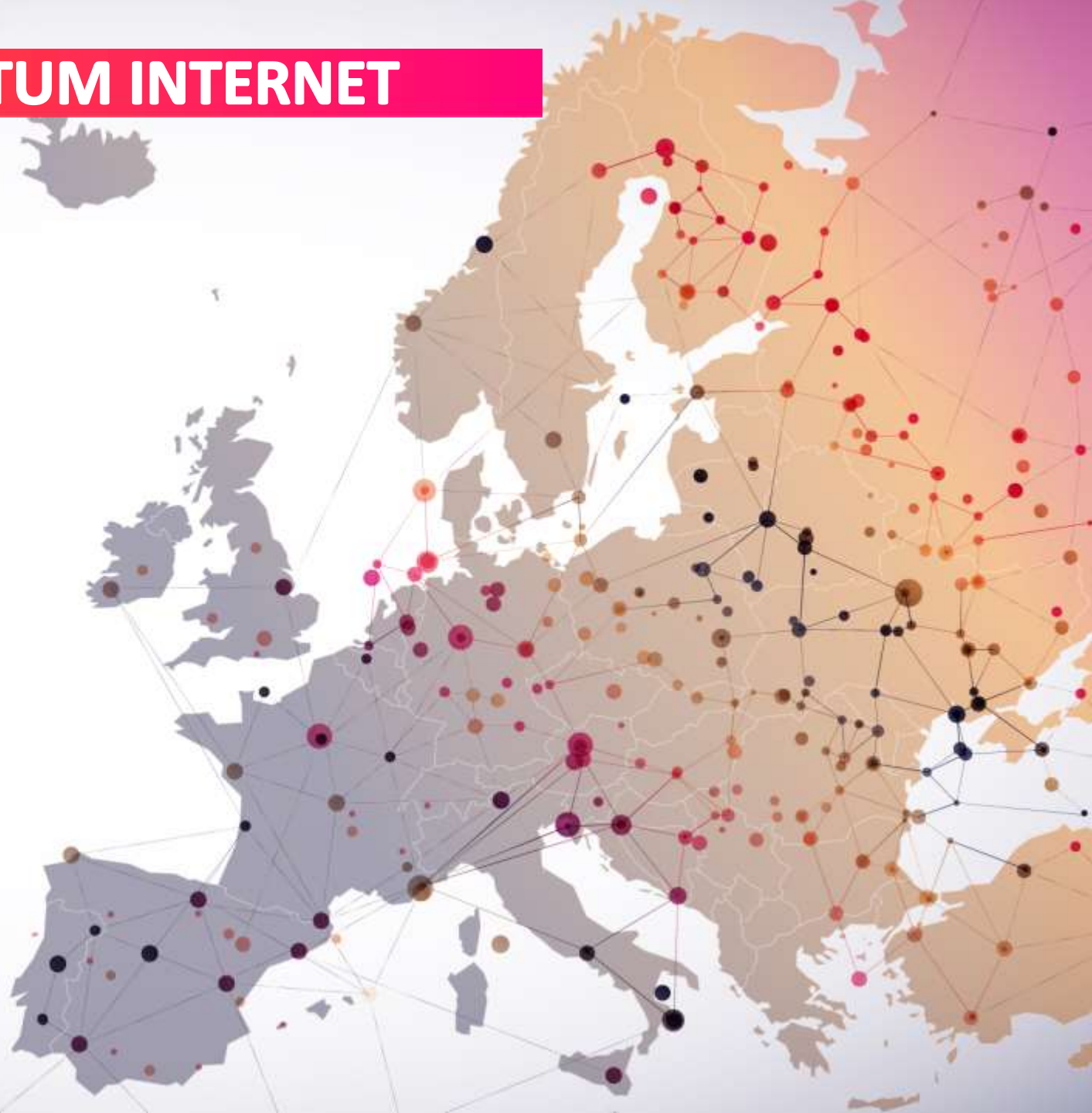
Kick-start a competitive European quantum industry

Make Europe attractive for innovation & investments



THE ULTIMATE GOAL: QUANTUM INTERNET





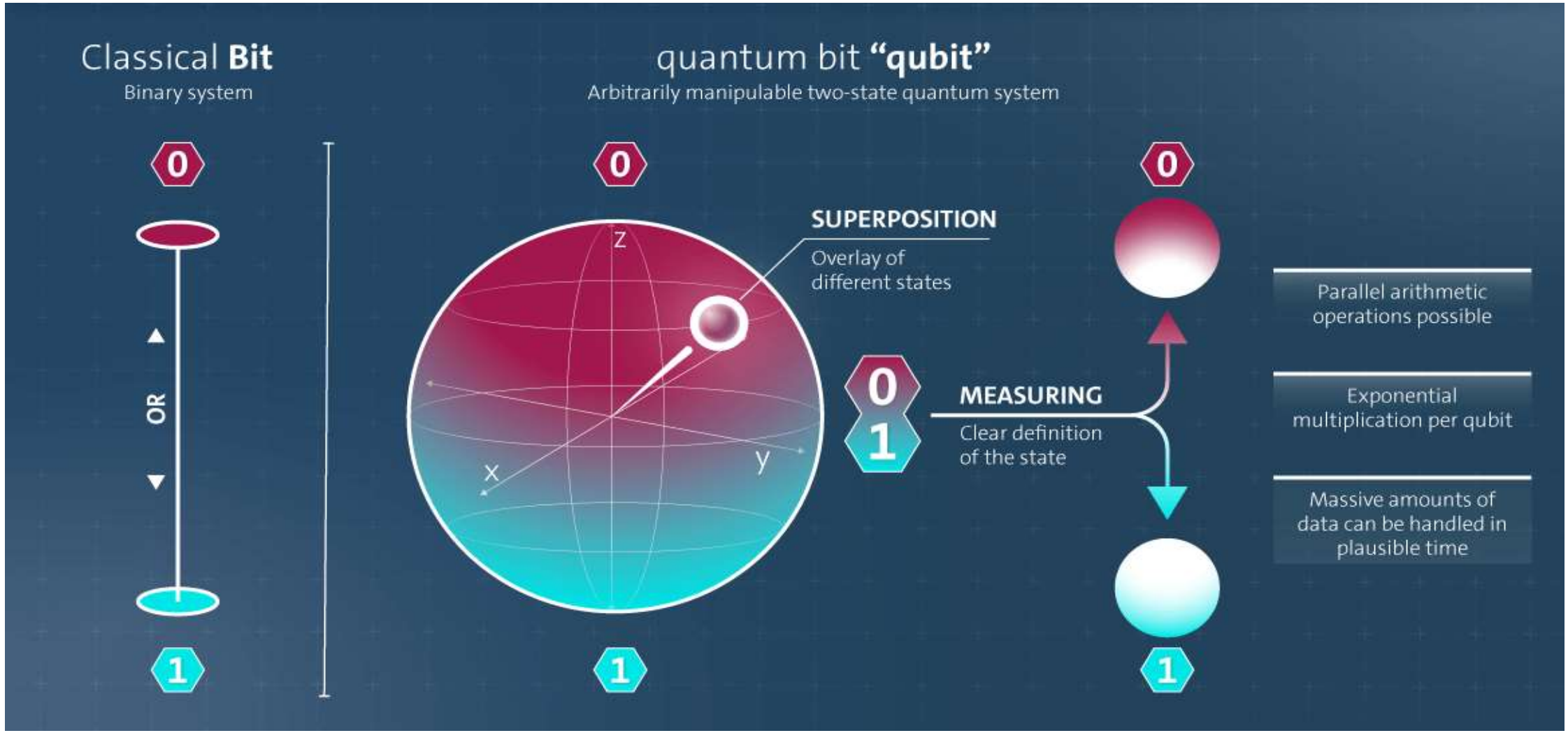

In collaboration
with Deloitte
WORLD
ECONOMIC
FORUM
Transitioning to a
Quantum-Secure Economy
WHITE PAPER
SEPTEMBER 2022


WORLD
ECONOMIC
FORUM
State of Quantum Computing:
Building a Quantum Economy
INSIGHT REPORT
SEPTEMBER 2022


THREATS
OPPORTUNITIES

What are the properties of a quantum computer?

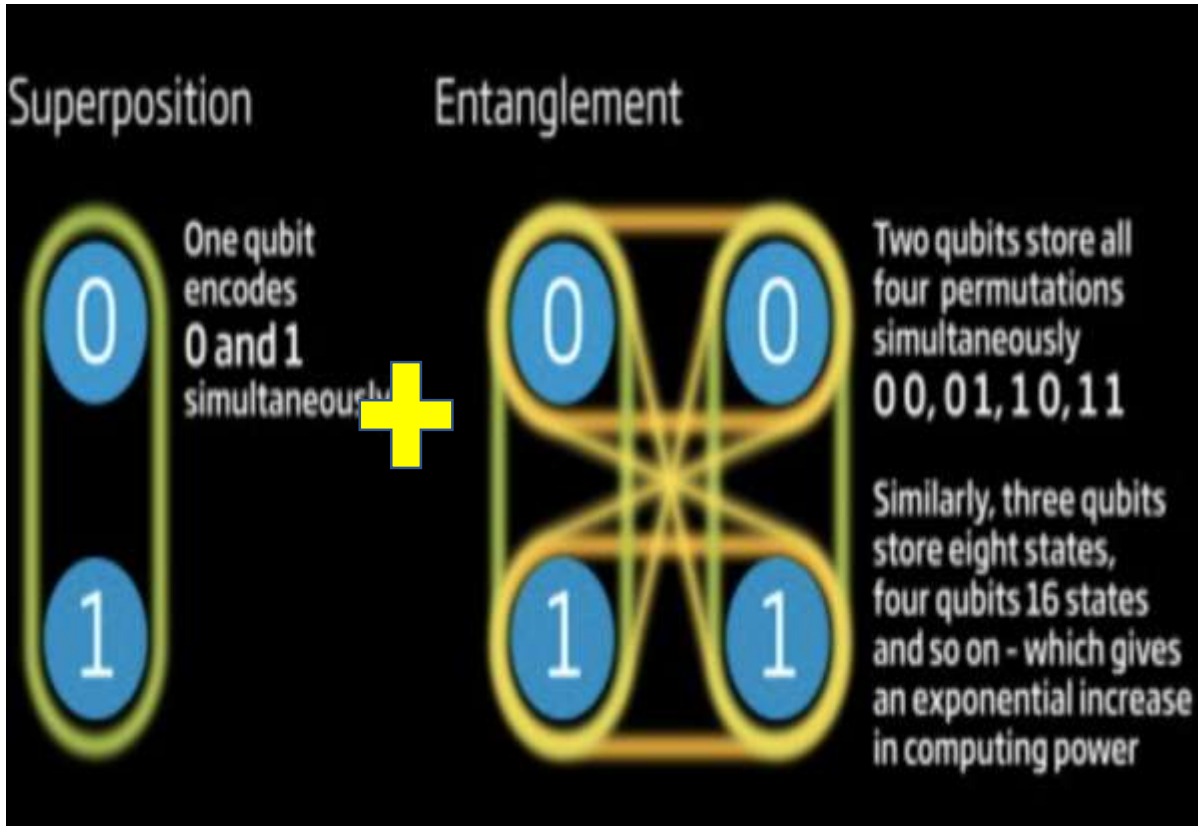
Current computers use bits but quantum computers use qubits.



Entanglement

- ***It thus appears that one particle of an entangled pair "knows" what measurement has been performed on the other, and with what outcome, even though there is no known means for such information to be communicated between the particles, which at the time of measurement may be separated by arbitrarily large distances***

- Its entanglement that gives quantum computing the ability to scale exponentially, as 2 entangled qubits can represent 4 states. The more linked qubits, the exponential increase in states and thus computing power.



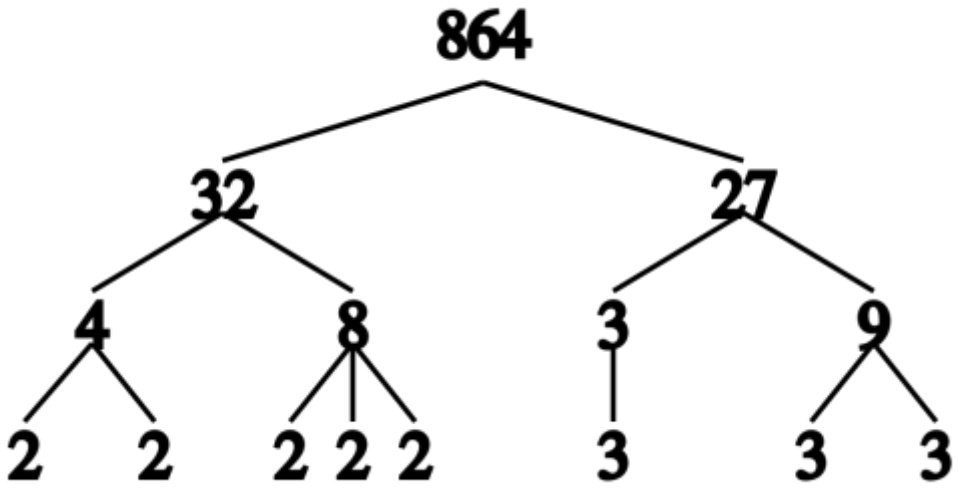
- 2^n states

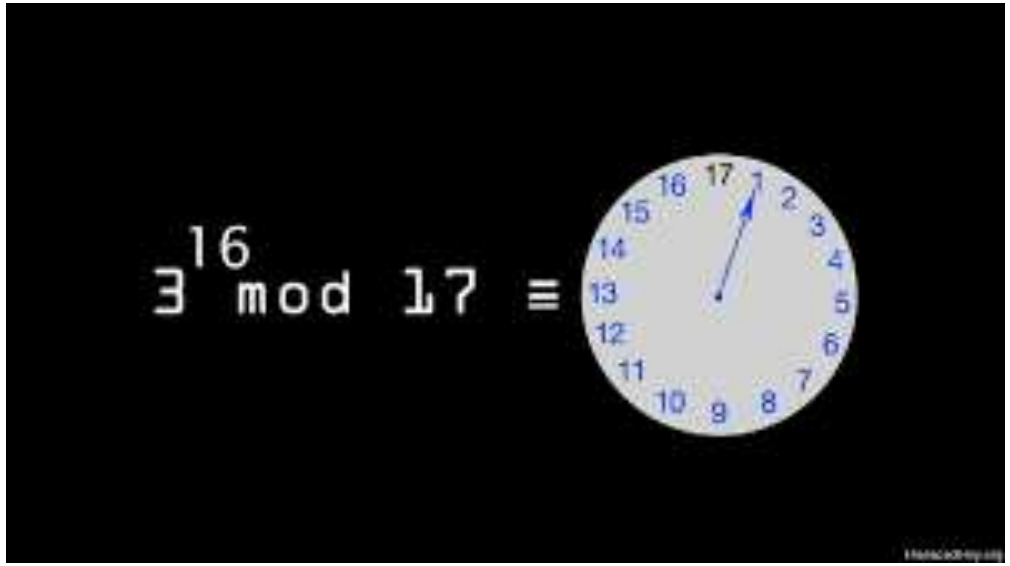
Fragility & No Cloning

A **quantum state** collapses to a classical state if disturbed by noise or measurement.

One **cannot** copy, intercept or steal without ruining a quantum state.

Src - IBM





Quantum computing threat to cryptography

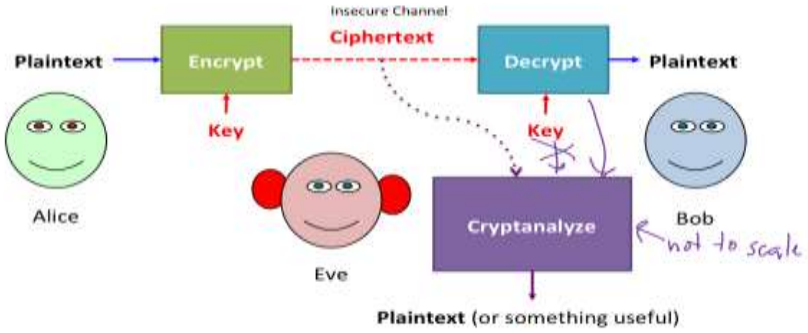
- Cryptography is based on 2 difficult math problems:
  - Integer Factorization
  - Discrete Log
- The strength of a one way function depends on the time needed to reverse it
- Meet Shor & Grover!

Requirements for individual privacy and global security

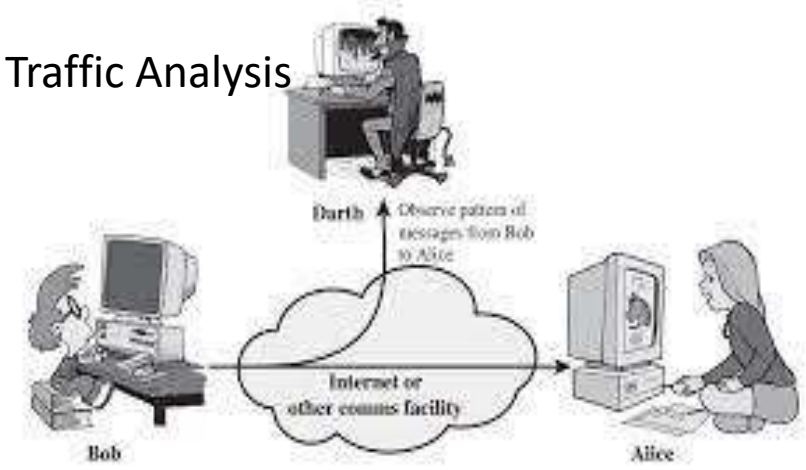
- *Secure Hardware*
- *Secure Operating Systems*
- *Secure Protocols*
- *Secure Applications*
- *Strong Cryptography*
- *Solid understanding of what you need to protect and from whom*

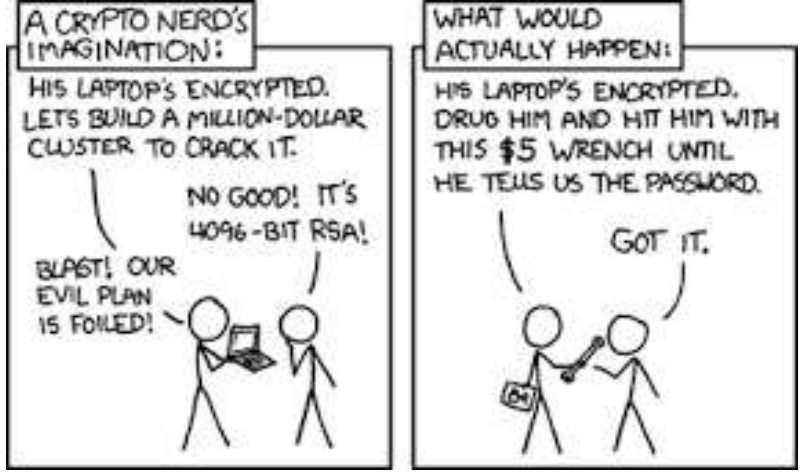
What can go wrong?

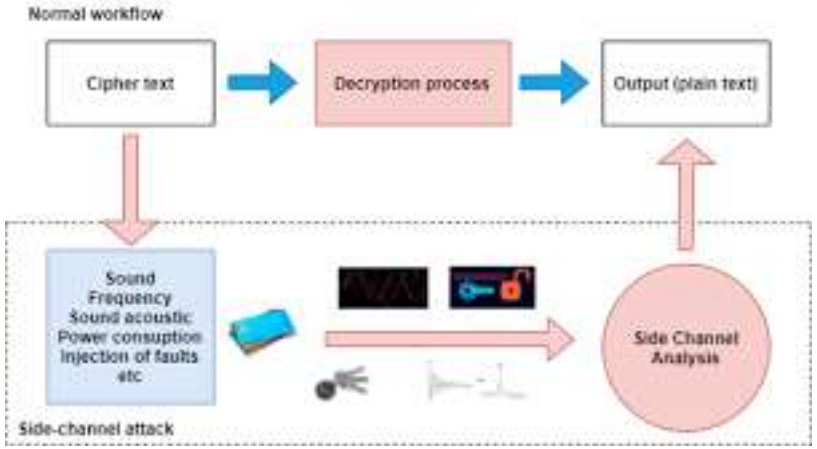
Cryptanalysis



Traffic Analysis



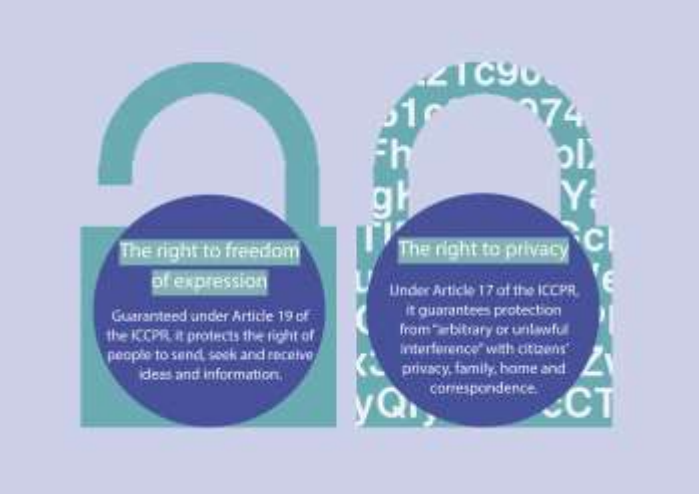


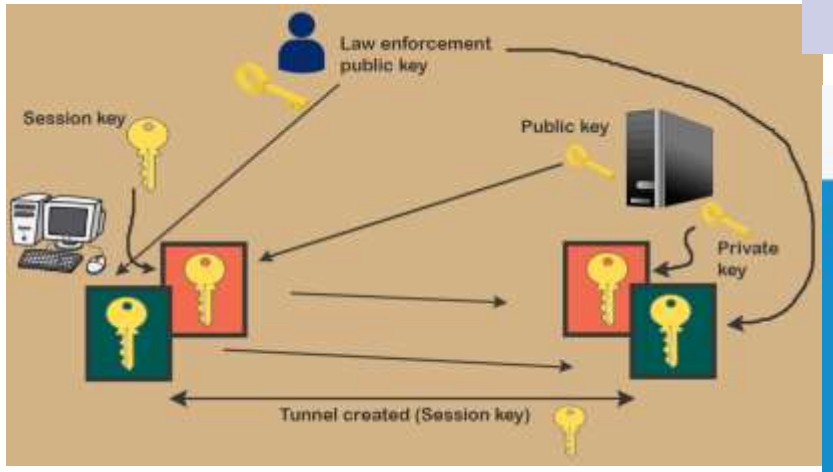


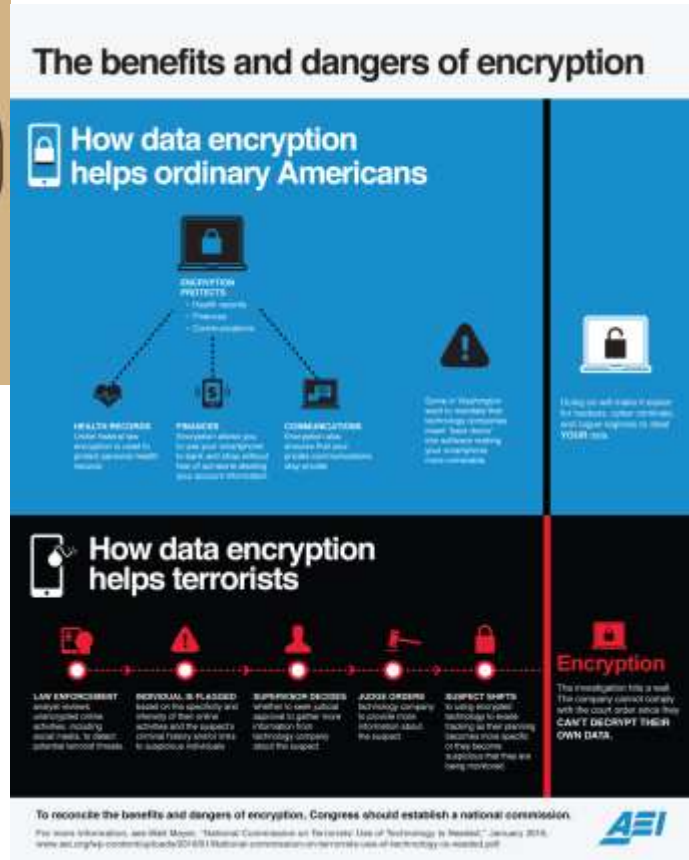
Balancing equities

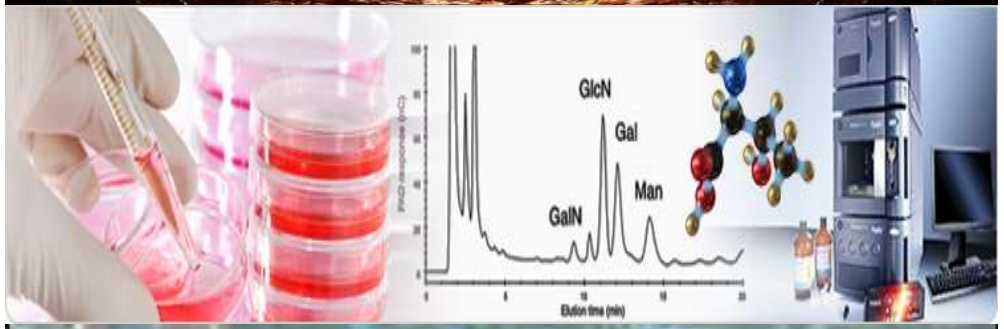
Arguments to weaken, ban, cryptography

- Cryptographic Export Restrictions
- Key Escrow Demands / Golden Key
- Key Management Considerations
- Enforcing Weakness / Algorithms
- Alternatives for Law Enforcement - Vulnerabilities and Zero Days ; Client Side Scanning







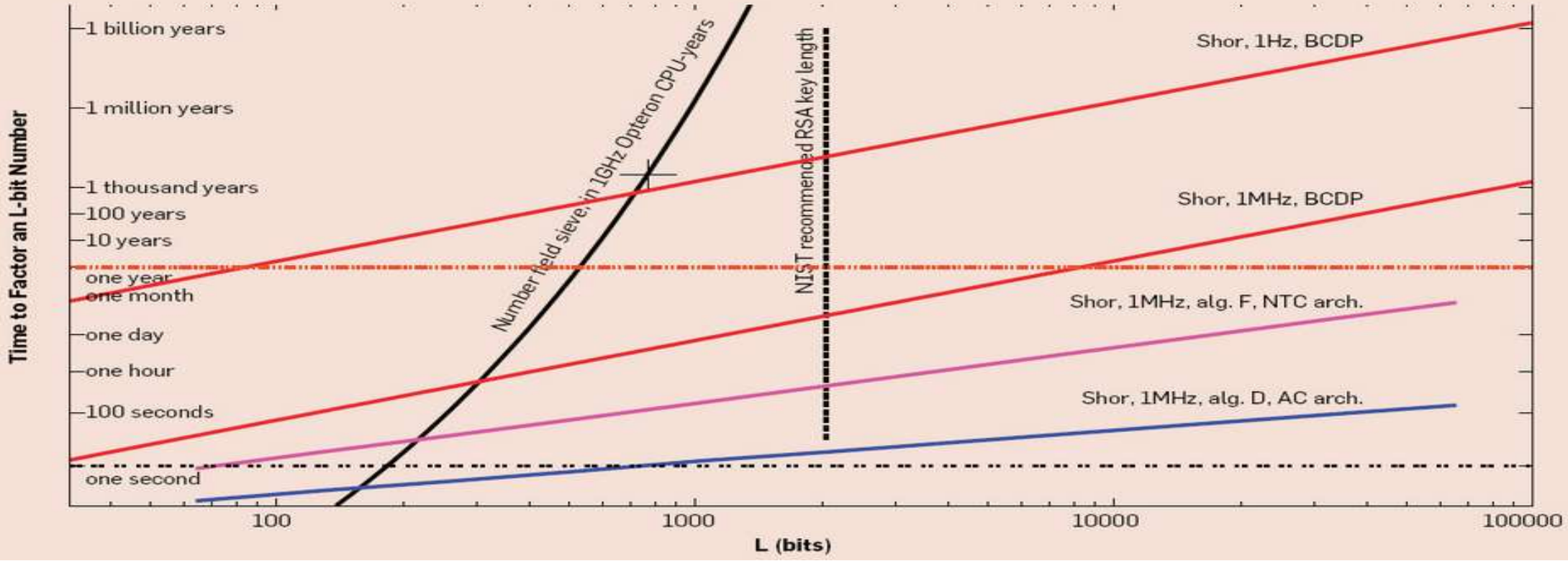


Power, Potential & Threat of a quantum computer

- How long do we need to keep our encryption secure?
- How long before there is a viable quantum computer that breaks our secrets?
- How long will we need to transition our network and systems to one that is quantum safe?

WHEN?

The horizontal axis is the length of the number to be factored. The steep curve is NFS, with the marked point at $L = 768$ requiring 3,300 CPU-years. The vertical line at $L = 2048$ is NIST's 2007 recommendation for RSA key length for data intended to remain secure until 2030. The other lines are various combinations of quantum computer logical clock speed for a three-qubit operation known as a Toffoli gate (1Hz and 1MHz), method of implementing the arithmetic portion of Shor's algorithm (BCDP, D, and F), and quantum computer architecture (NTC and AC, with the primary difference being whether or not long-distance operations are supported). The assumed capacity of a machine in this graph is $2L^2$ logical qubits. This figure illustrates the difficulty of making pronouncements about the speed of quantum computers.



Prioritizing Important before its Urgent

c|net COVID-19 BEST REVIEWS NEWS HOW TO SMART HOME CARS

IBM promises 100x faster quantum computers through new software foundations

Big Blue's open-source software efforts span the basics of quantum computing to higher-level jobs like AI and molecular simlutations.

Stephen Shankland Feb. 3, 2021 10:24 p.m. PT ▶ LISTEN · 02:40

CCC
Computing Community Consortium
Catalyst

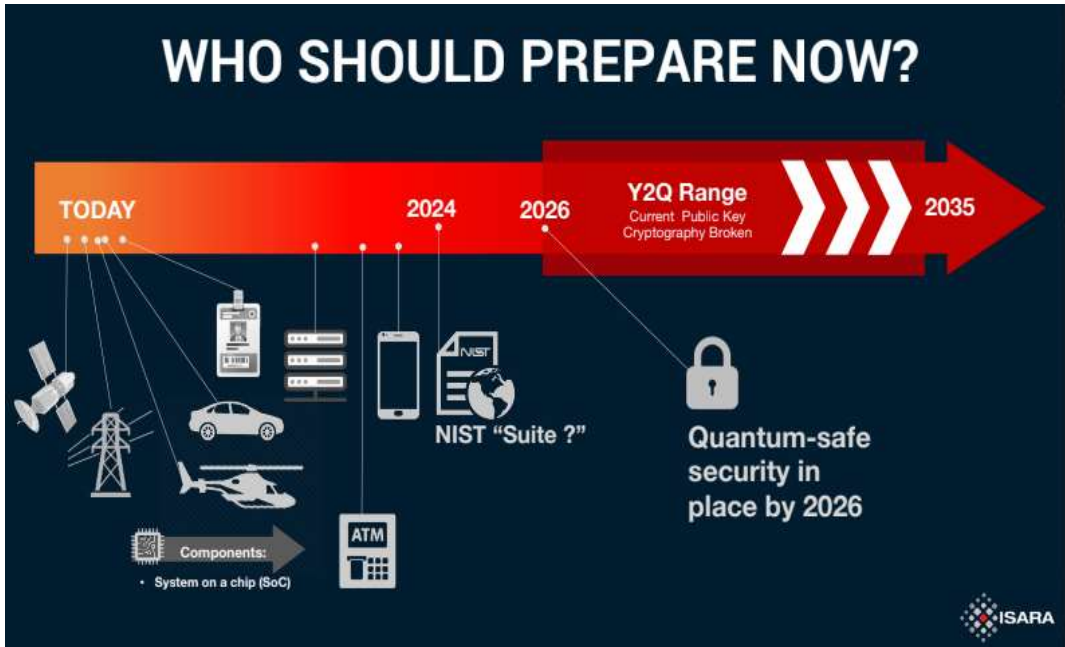
Post Quantum Cryptography: Readiness Challenges and the Approaching Storm

A Computing Community Consortium (CCC) Quadrennial Paper

Matt Campagna (Amazon), Brian LaMacchia (Microsoft Research), and David Ott (VMware Research)

Introduction

https://cra.org/ccc/resources/ccc-led-whitepapers/#2020-quadrennial-papers



Capture Now, Decrypt later

The predictive force of old secrets means that you can not only see what you have done, but what you're planning on doing

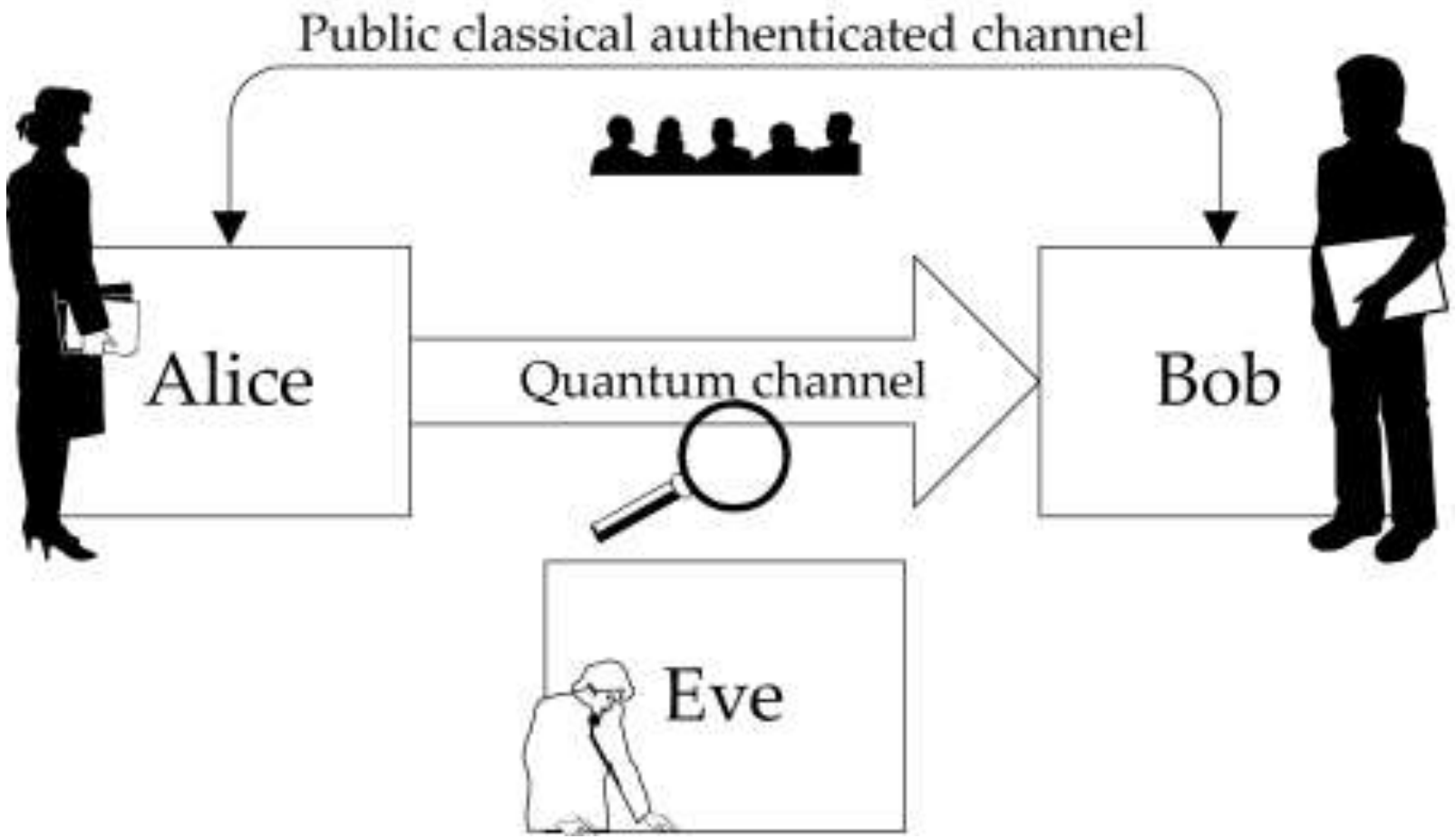
Phased plan of defense

- *Increase Key Length of Current Crypto used*
- *Investigate options for Quantum Key Distribution*
- *Investigate Post Quantum Algorithms*

Impact ?

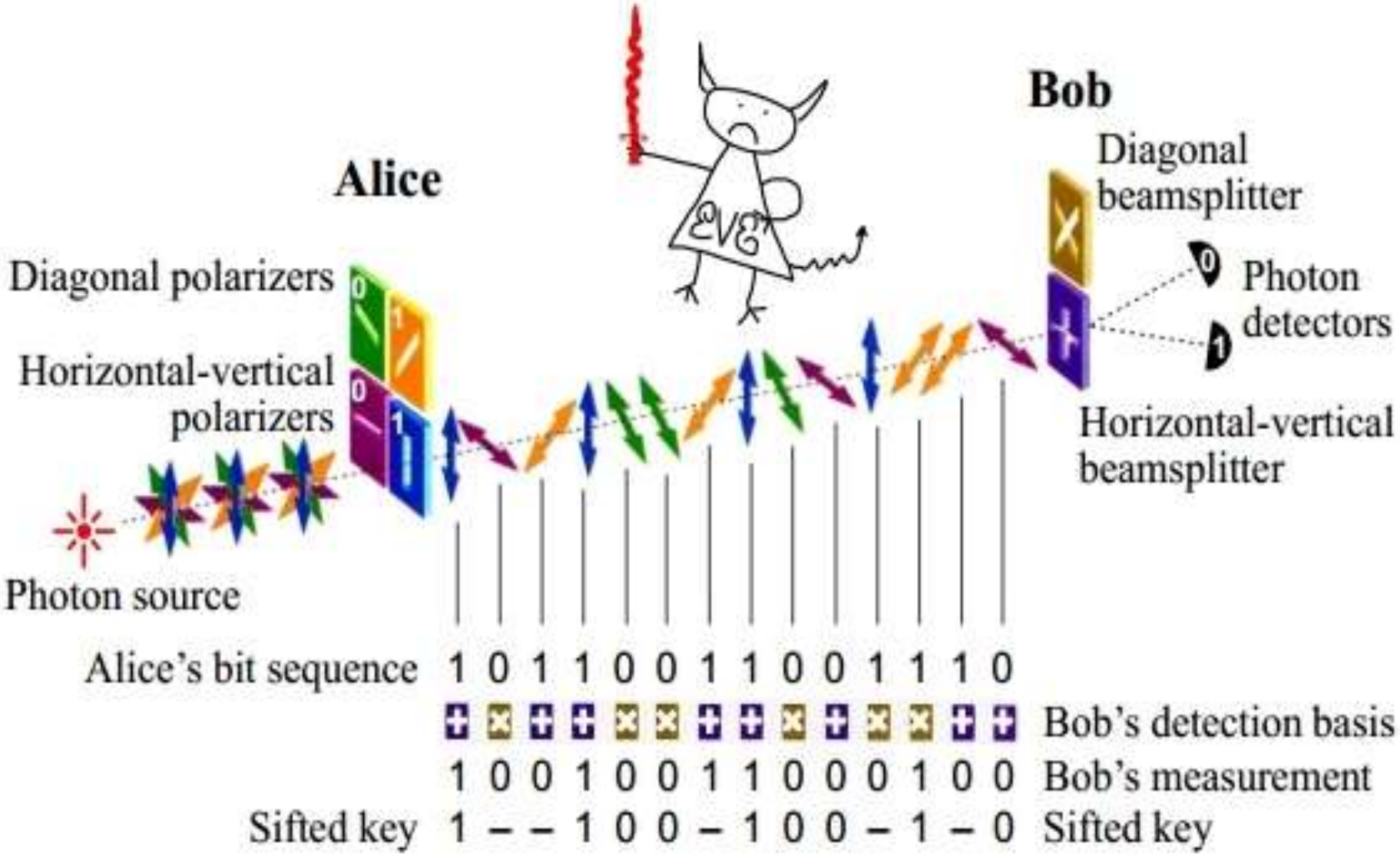
Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES-256	Symmetric key	Encryption	Larger key sizes needed
SHA-256, SHA-3		Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms



Quantum Key Distribution

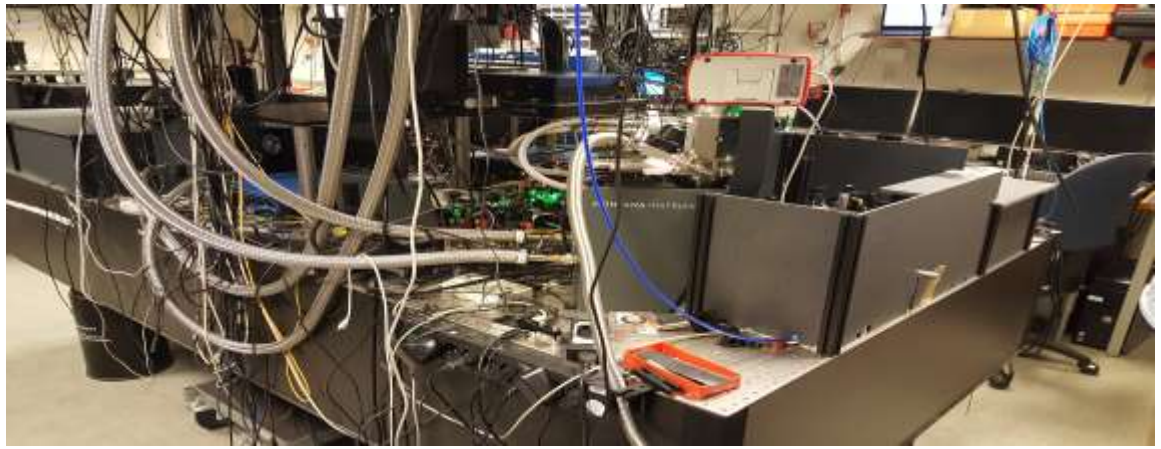
QKD -


Alice
Bob
EVE
Diagonal polarizers
Horizontal-vertical polarizers
Photon source
Diagonal beamsplitter
Photon detectors
Horizontal-vertical beamsplitter
Alice's bit sequence 1 0 1 1 0 0 1 1 0 0 1 1 1 0
Bob's detection basis
1 0 0 1 0 0 1 1 0 0 0 1 0 0 Bob's measurement
Sifted key 1 – – 1 0 0 – 1 0 0 – 1 – 0 Sifted key

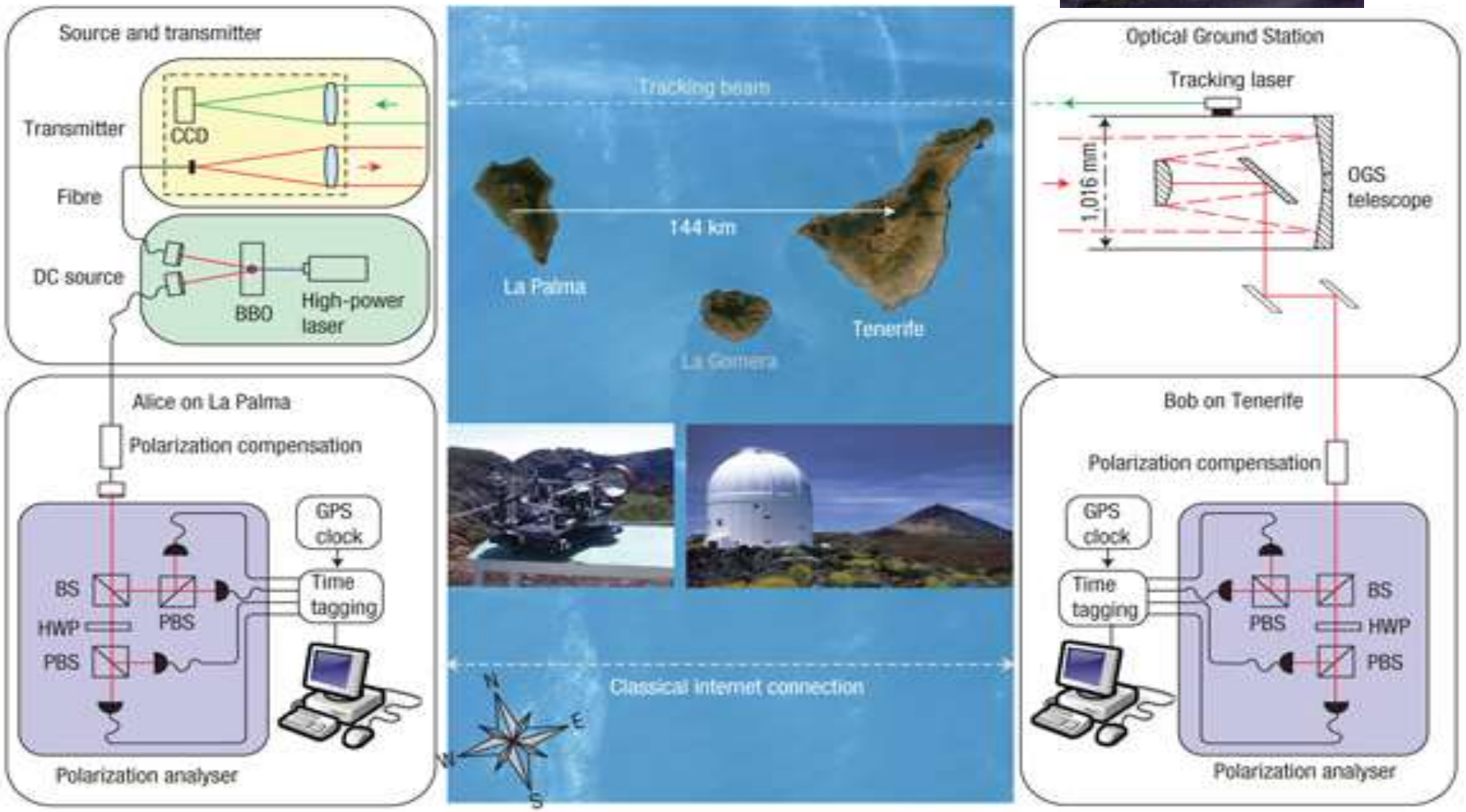
KPN’s Quantum leap with IDQuantique

NL Quantum Internet Backbone

NL Quantum Internet Backbone – Step 1 – Delft & DH
QUTECH - TUDELFT



Free Space QKD



PQC Reaches an Inflection Point

2016
Public call for candidate submissions
- 82 received

2017
Round 1 completed
- Whittled down to 69 algorithms
- 21 broken

2019
Round 2 completed
- 26 algorithms remain
- 8 suffered attacks

2021
Round 3 completed
- 7 finalists selected
- 1 suffered attack

2022
- 4 finalists expected to be announced in early 2022
- Call for public comments opens

2024
Standard finalized

2025–26
Commercial products using approved algorithms begin to hit the market

2034+
NIST warns 5–15 years will be needed after final standards are published for full transition to be completed

Post Quantum Crytographic Algorithms

- Onto Round 4 -

	Finalists	Alternates
KEMs/Encryption	Kyber NTRU SABER Classic McEliece	Bike FrodoKEM HQC NTRUprime SIKE
Signatures	Dilithium Falcon Rainbow	GeMSS Picnic SPHINCS+

SIKE!

NIST Post-Quantum Algorithm Finalist Cracked Using a Classical PC

By Kevin Townsend on August 10, 2022

Share Tweet RSS

An algorithm submitted to the NIST post-quantum encryption competition - and one that made it to the fourth round - has been defeated. The algorithm, Supersingular Isogeny Key Encapsulation (SIKE), was broken by Wouter Castryck and Thomas Decru at KU Leuven, and

Post-quantum WireGuard

June 16, 2021

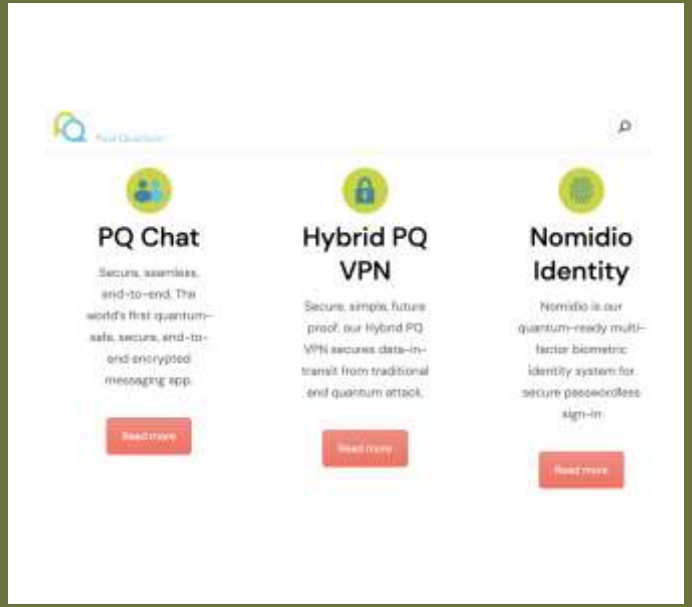
Andreas Hülsing
Eindhoven University of Technology
The Netherlands
andreas@huelsing.net

Kai-Chun Ning
KPN B.V.
The Netherlands
kaichun.ning@kpn.com

Peter Schwabe
Max Planck Institute for Security and Privacy, Germany &
Radboud University, The Netherlands
peter@cryptojedi.org

Florian Weber
Eindhoven University of Technology
The Netherlands
mail@florianjw.de

Philip R. Zimmermann
Delft University of Technology & KPN B.V.
The Netherlands
prz@mit.edu



Readying implementation for Daily Use

Post Quantum Cryptography

- Inventory of crypto assets
- Think it through for implementation readiness
- Look for crypto agility and opportunities
- Create Policies for innovation areas
- Engage with HW & SW vendors
- Supplier Security Annex
- Start Failing early !

2016 - China launched the world's 1st Quantum Communications Satellite

"China is completely capable of making full use of quantum communications in a regional war. The direction of development in the future calls for using relay satellites to realize quantum communications and control that covers the entire army."

Professor Pan Jianwei

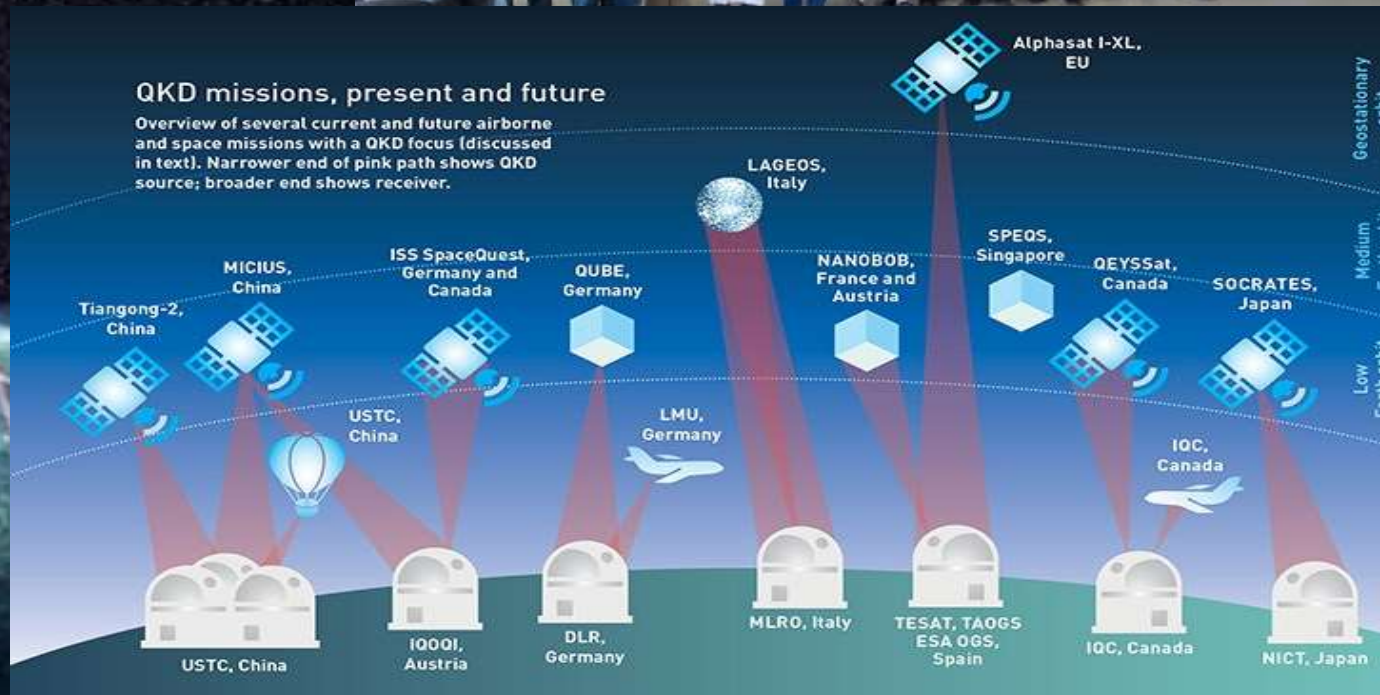
University of Science and Technology of China

+10bn QIS +AliBaba

Micius -


Retired research chimps stuck in limbo
Job losses undermine educational advancement
Marine predators shape prey defenses
Science
$15
16 JUNE 2017
AAAS
QUANTUM
REACH
Entangled photon pairs sent from space to Earth
pp. 1110 & 1140


Optical aircraft terminal
Main terminal controller
Optical ground station
Canada


QKD missions, present and future
Overview of several current and future airborne and space missions with a QKD focus (discussed in text). Narrower end of pink path shows QKD source; broader end shows receiver.
Alphasat I-XL, EU
LAGEOS, Italy
SPEOS, Singapore
QEYSSat, Canada
SOCRATES, Japan
NANOBOB, France and Austria
ISS SpaceQuest, Germany and Canada
QUBE, Germany
MICIUS, China
Tiangong-2, China
USTC, China
LMU, Germany
IQC, Canada
Geostationary
Medium
Low
USTC, China
IQOQI, Austria
DLR, Germany
MLRO, Italy
TESAT, TAOGS ESA OGS, Spain
IQC, Canada
NICT, Japan

Space Based QKD

- Bridge between terrestrial repeaters
- Additional Gains (C, I, A)
- Mitigating risks?
- Finding the right use cases

Qritical

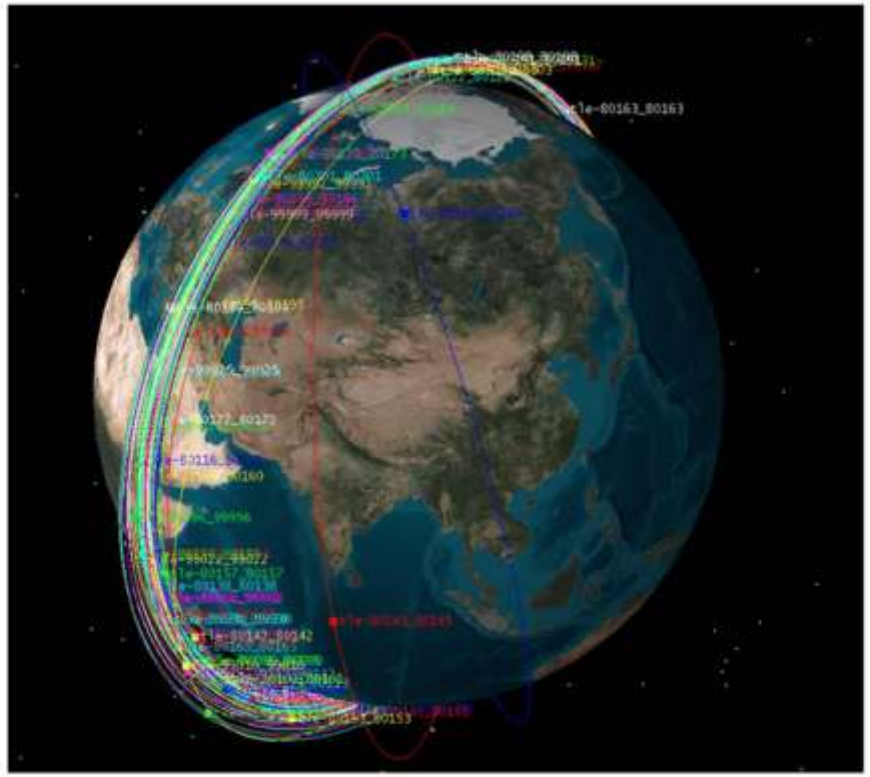
Final Presentation

kpn ABN·AMRO TNO innovation for life CGI

Experience the commitment®

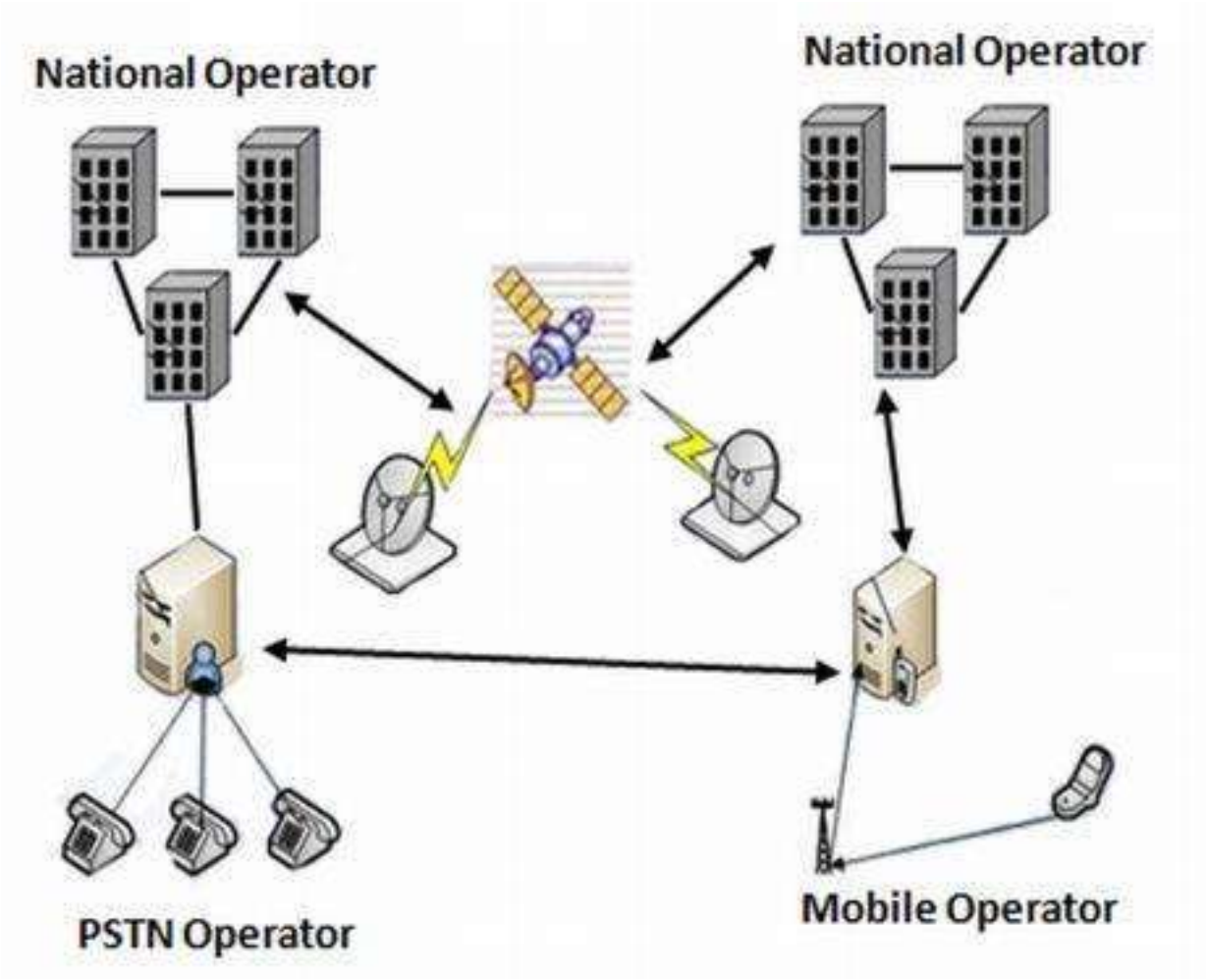
A-SAT & other, more recent events

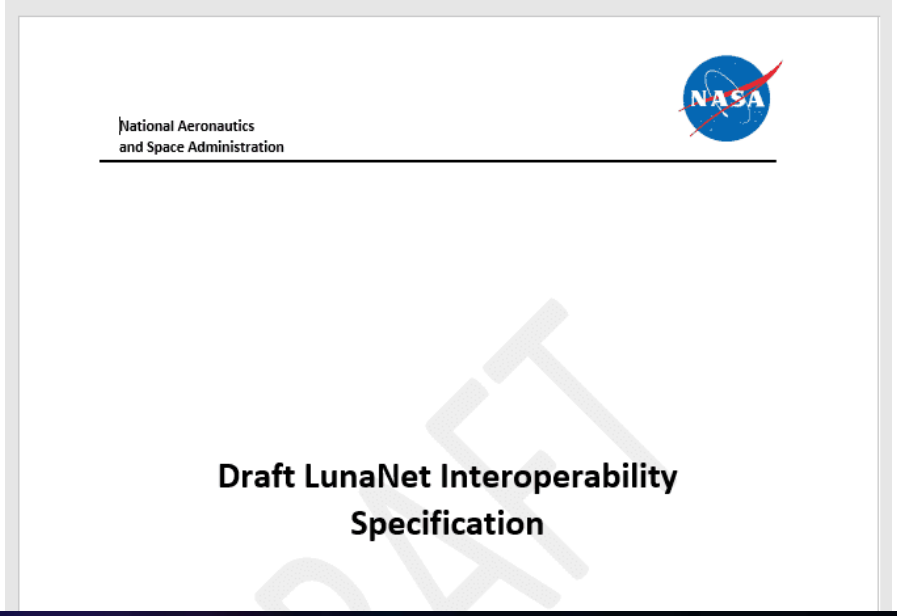
Threat Models are changing



3D graph of the cloud of tracked fragments as of 18 November 2021

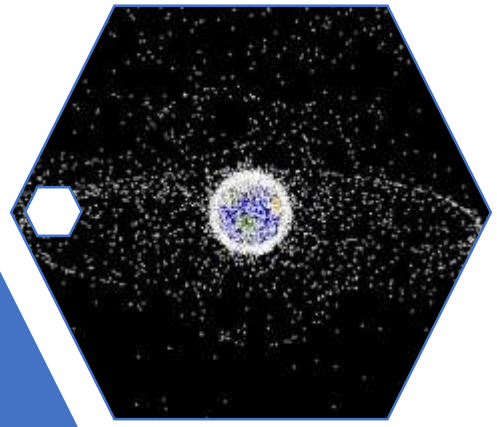
For Sharing Infrastructure ?





FOR INTERCONNECT & BILLING ?

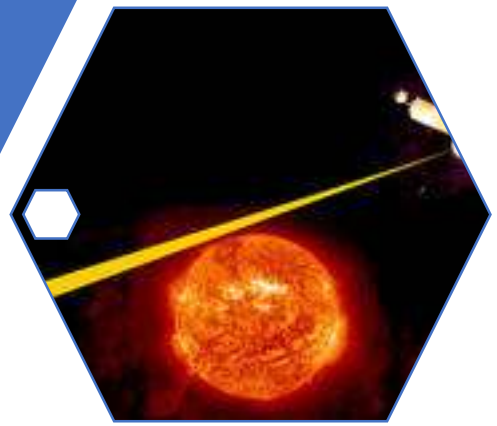
Lots of moving parts…



(Cyber) Resilience

Crypto Agility

Supply Chain Security



Starlink & Amara’s Law

Ondrej Vlcek

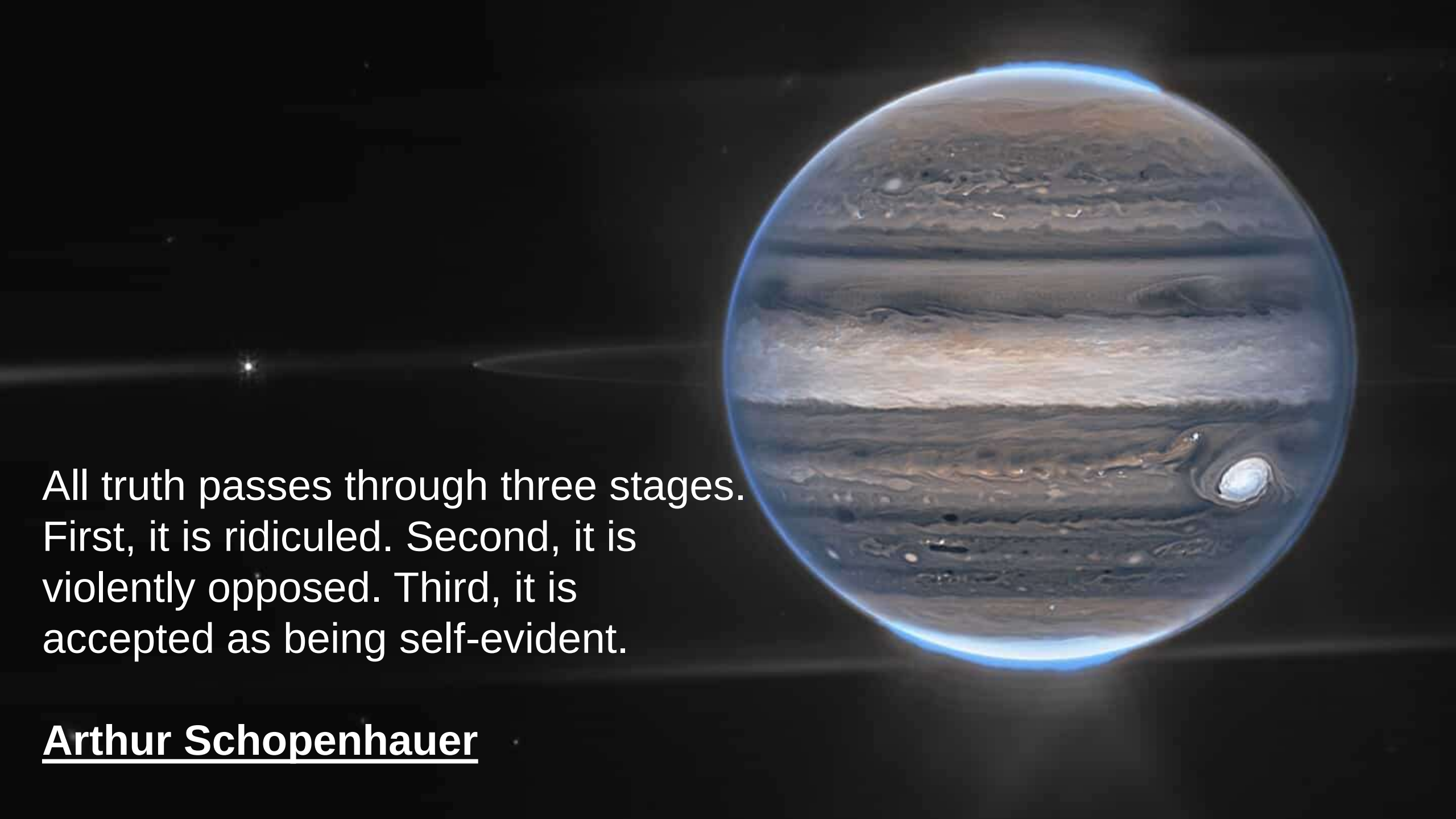
CEO at Avast

View full profile

install Starlink in my remote retreat, where connectivity of any kind has always been a problem. And boy, it’s working like a charm! Amazing! 🙏😊

And while I am now reflecting on it, this little anecdote again reminded me of Amara’s Law that says that we tend to overestimate the effect of technology in the short run and underestimate its effect in the long run. So true. I mean, just think about what telecommunications may look like in the next 30 years!

#technology #connectivity #starlink #amazingfuture



All truth passes through three stages. First, it is ridiculed. Second, it is violently opposed. Third, it is accepted as being self-evident.

Arthur Schopenhauer

Avast

THANK YOU.

Jaya Baloo. **@jayabaloo**