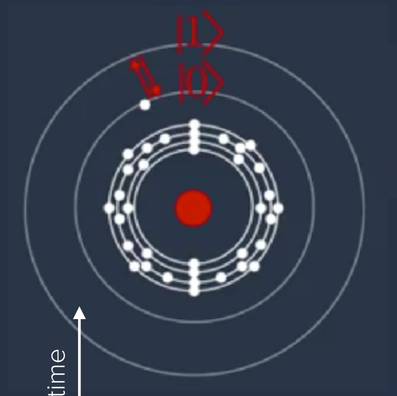
Comunicación Cuántica, Retos y Oportunidades para las empresas

Jornades EIC - Comunicacions i Seguretat en la revolució quàntica

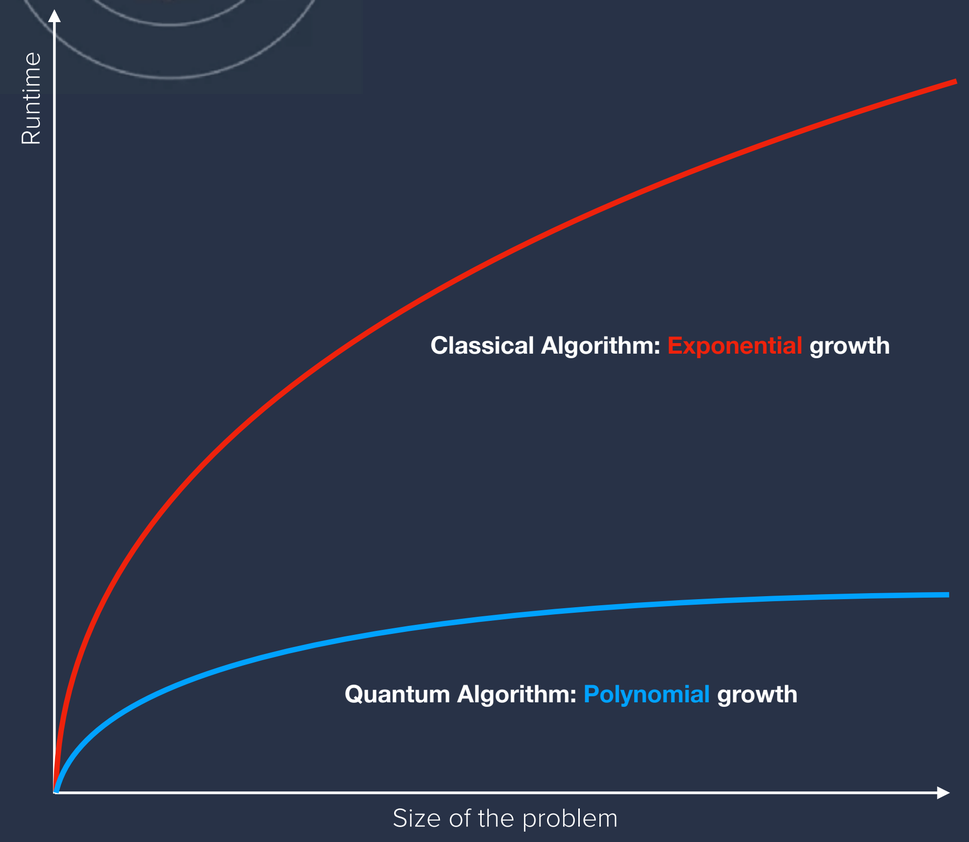
Pau Velando, maig 2021

Un nuevo modelo de amenza a la seguridad digital como la conocemos hoy



Superposition

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$



100 transistors

100 bits

1 state of 100 bits, at a time

RSA-2048: ~ 1 billion years

100 atoms

100 qubits

1267650600228229401496703205376

= 10^{30} states, at a time

RSA-2048: ~ 1 hour

Un nuevo modelo de amenza a la seguridad digital como la conocemos hoy:

La criptografía basada en el intercambio de claves públicas

RSA-100, 100 decimal digits (330 bits)

RSA-100 = 15226050279225333605356183781326374297180681149613806886579084945801229632589528976540003506920061 39

RSA-100 = 37975227936943673922808872755445627854565536638199 × 40094690950920881030683735292761468389214899724061

RSA-640, 193 decimal digits (640 bits)

RSA-640 = 3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609

RSA-640 = 1634733645809253848443133883865090859841783670033092312181110852389333100104508151212118167511579 × 1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571

--- not factored, yet ---

RSA-260, 260 decimal digital (862 bits)

2211282552952966643528108525502623092761208950247001539441374831912882294140200198651272972656974659908590033003140005117074220456085927635795375718595429883895870922923849100670303412462054578456641366454068421436129301769402084639106587591479425143514445819 9

RSA-1024, 309 decimal digits (1024 bits)

1350664108659952233496032162788059699388814756056670275244851438515265106048595338339402871505719094417982072821644715513736804197039641917430464965892742562393410208643832021103729587257623585096431105640735015081875106765946292055636855294752135008528794163773285339061097505443349998111500569772368909275 63

RSA-2048, 617 decimal digits (2048 bits)

2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440691829064124951508218929855914917618450280848912007284499268739280728777673597141834727026189637501497182469116507761337985909570009733045974880842840179742910064245869181719511874612151517265463228221686998754918242243363725908514186546204357679842338718477444792073993423658482382428119816381501067481045166037730605620161967625613384414360383390441495263443219011465754445417842402092461651572335077870774981712577246796292638635637328991215483143816789988504044536402352738195137863656439121201039712282212072035 7

Las propiedades cuánticas de la materia: amenaza y oportunidad

2 alternativas para las empresas

Mathematics

Quantum-resistant cryptography (post-quantum)

Quantum-resistant algorithms are implemented on existing platforms and derive their security through **mathematical complexity.** Standard communications with quantum-resistant cryptography. Not yet...

Physics

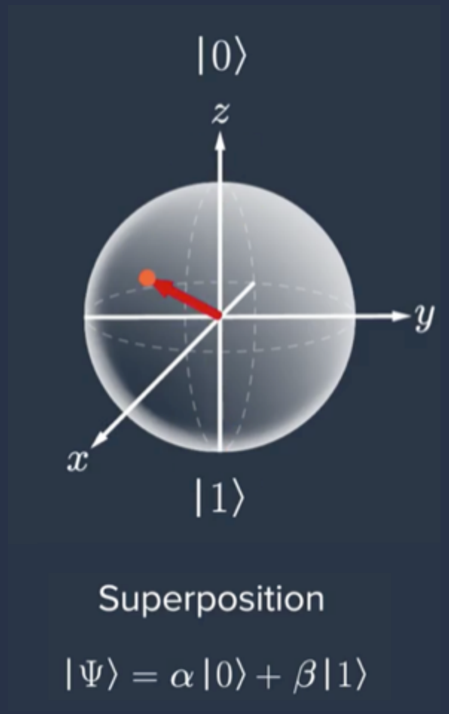
Random Numbers Generation

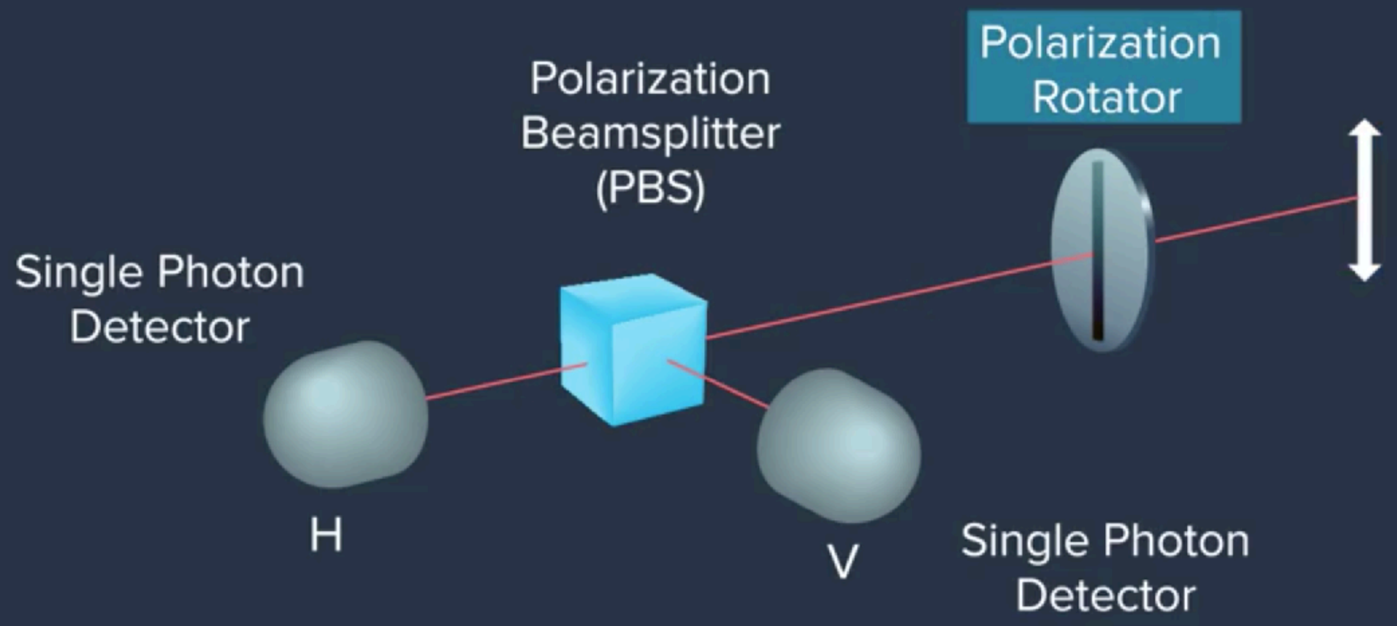
Quantum Key Distribution (QKD)

Quantum key distribution utilizes the unique properties of **quantum mechanical** systems to generate and distribute cryptographic keying

NSA - National Security Agency, https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/

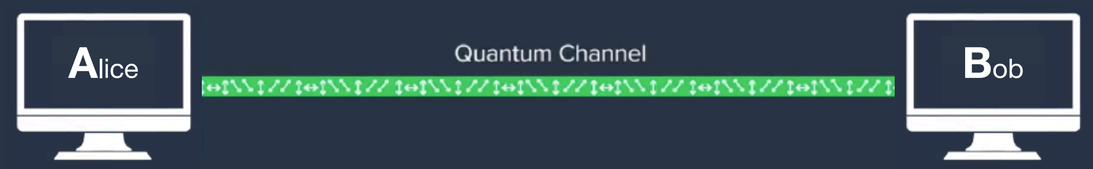
QKD, el intercambio de claves cuánticas: el principio

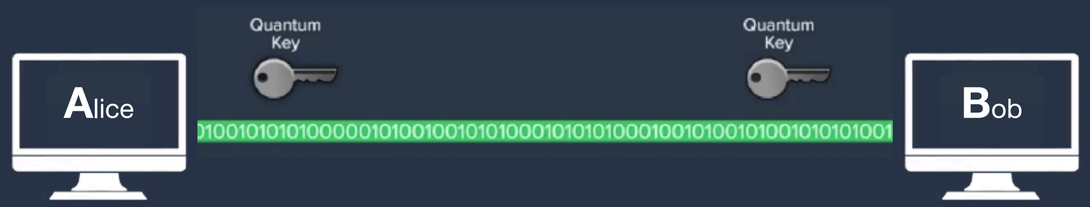


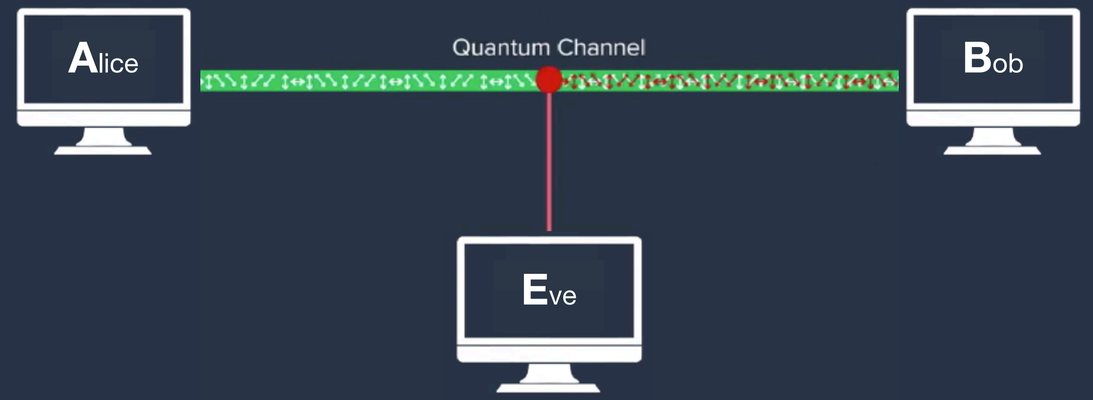


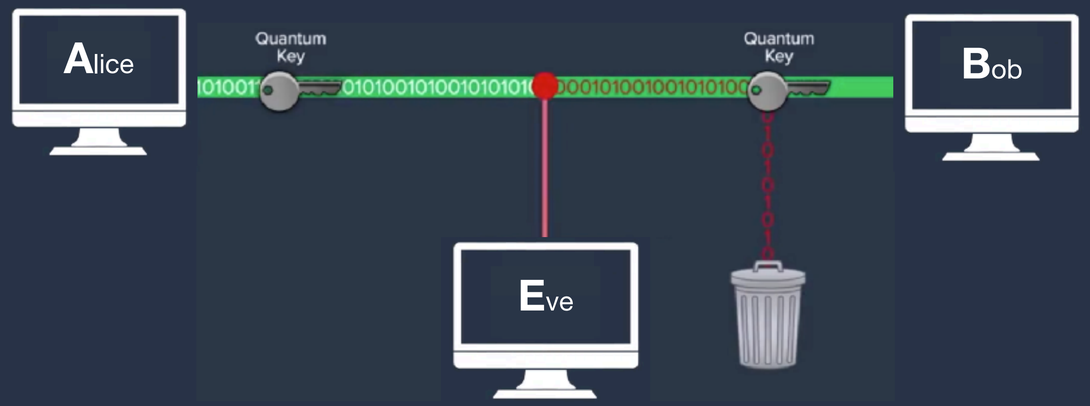
Source: MIT, Aplications of quantum computers

QKD, el intercambio de claves cuánticas: el principio



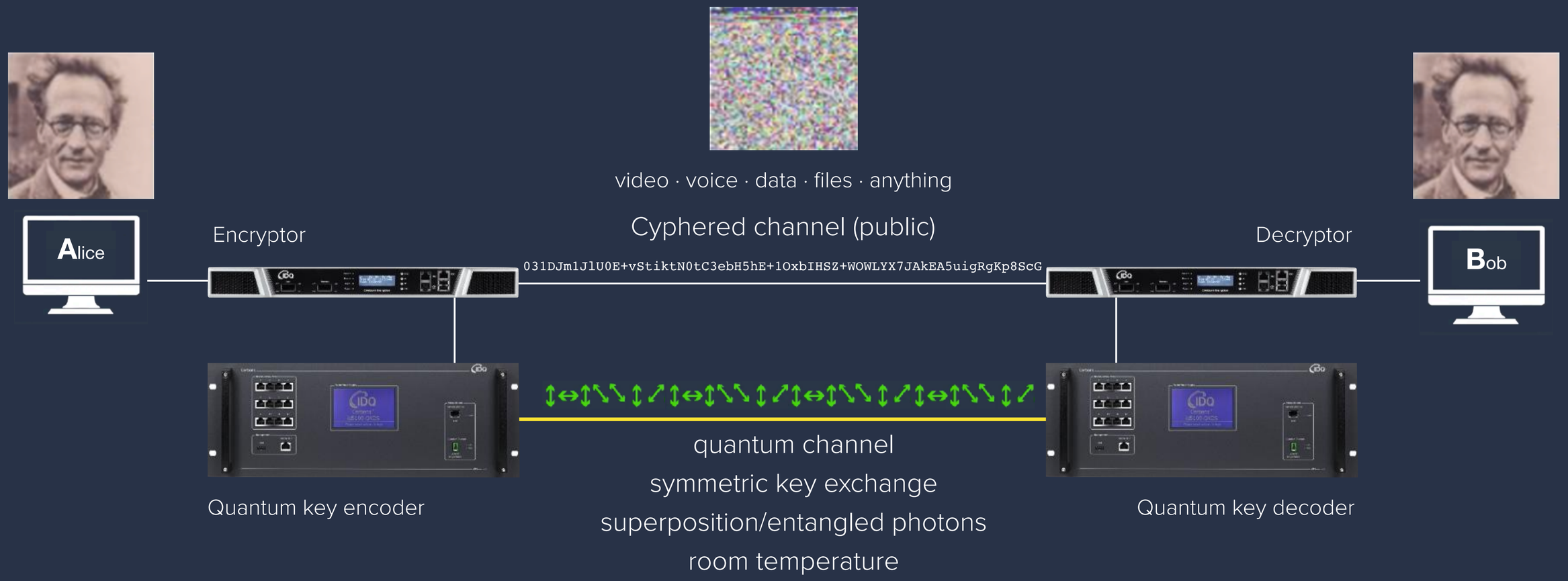




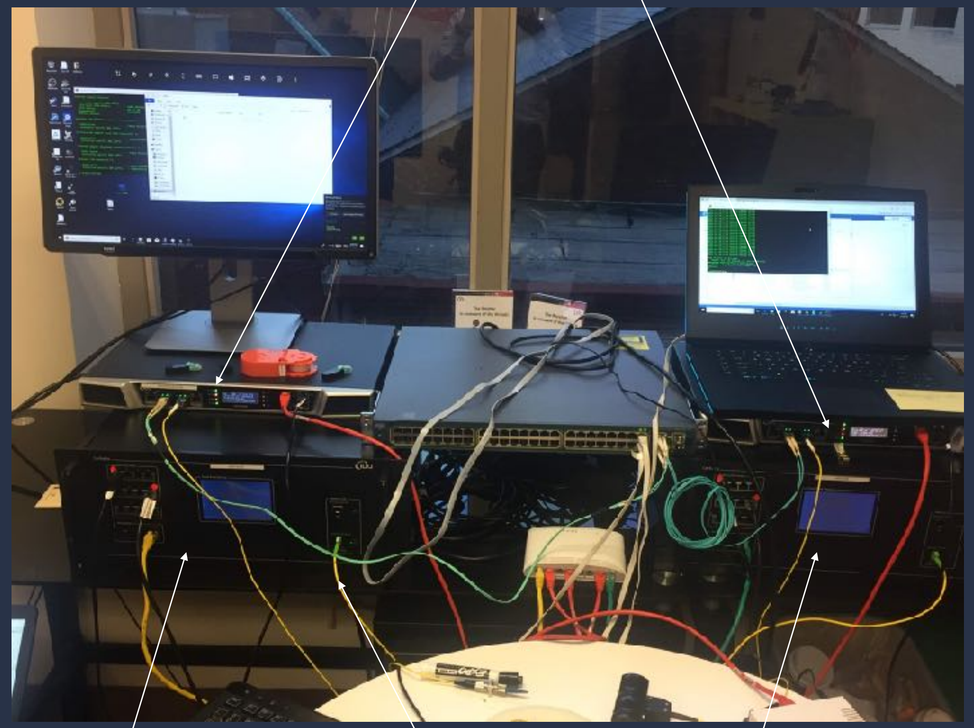


Source: MIT, Aplications of quantum computers

QKD, el intercambio de claves cuánticas: la práctica



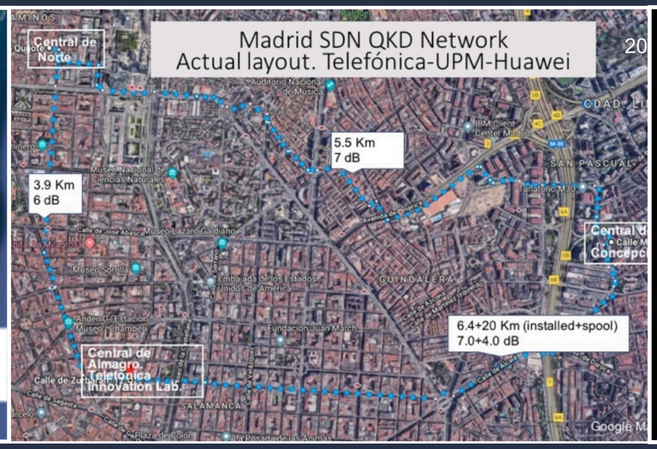
QKD, el intercambio de claves cuánticas: la práctica



Años de experiencias

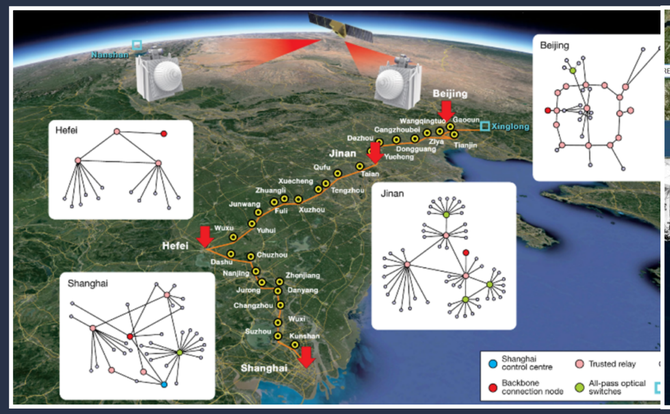
ICFO - CTTI, 2017, 30km

Madrid, 2018



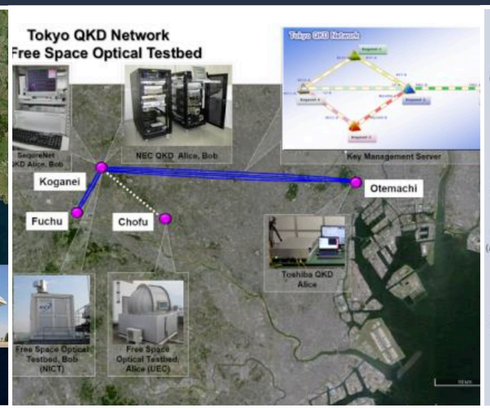
China - Europe, 2018, 7.600km

China, multi-mode, 2021



Italy, 2016, 1.700km

Tokyo, 2016

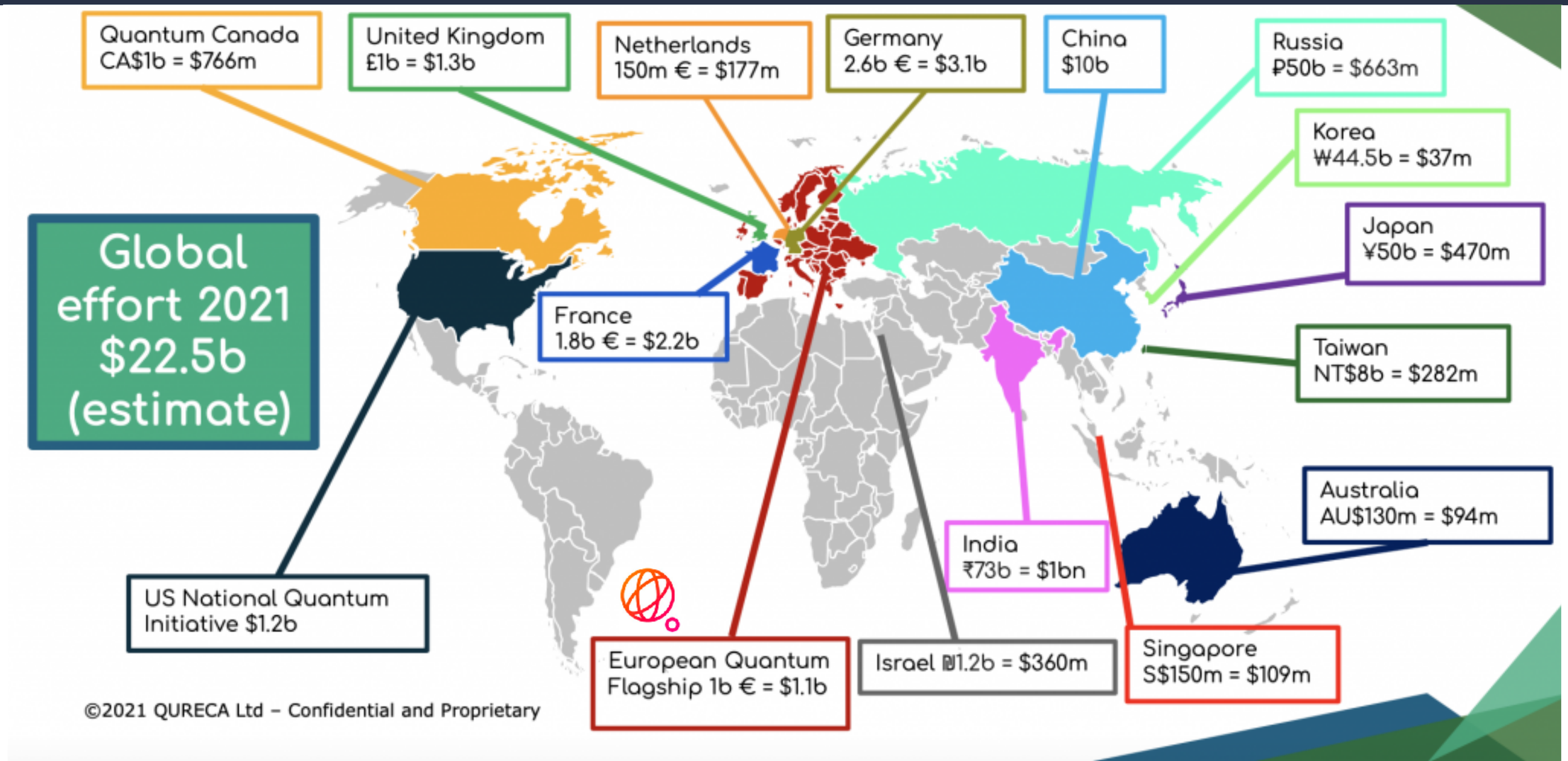


USA, 2018

Korea, 2015-20

Inversiones en tecnologías cuánticas

(Comunicación, computación, sensores y simulación)



Escenarios de inversión en Europa

Top Cities (#Startups)		
1.	London	8
2.	Paris	4
3.	Berlin, Cambridge	3
4.	Barcelona, Helsinki, Innsbruck, Lausanne, Munich, Oxford	2

Top Countries (#Startups)		
1.	UK	23
2.	Germany	13
3.	France	7
4.	Spain, Switzerland	4
5.	Finland, The Netherlands	3

Top Cities (Cumulated Funding)		
1.	Cambridge	€51.1m
2.	Espoo	€26.5m
3.	Tel Aviv	€19.5m
4.	Rorschach	€10.0m
5.	London	€9.4m

Top Countries (Cumulated Funding)		
1.	UK	€84.8m
2.	Finland	€26.7m
3.	Israel	€19.5m
4.	Switzerland	€12.4m
5.	France	€2.9m

UK startups raised the most funding (€85m), followed by Finland (€27m), Israel (€20m), and Switzerland (€12m). Quantum computing startups in France (€3m)

Cambridge Quantum Computing (€44.3m; Cambridge, UK), IQM (€26.5m; Espoo, Finland), Quantum Machines (€19.5m; Tel Aviv, Israel), Terra Quantum (€10.0m; Rorschach, Switzerland), and Quantum Motion Technologies (€8.7m; Leeds, UK).

UNTERNEHMERTUM VENTURE CAPITAL

@alex_kiltz

13-oct-2020

https://medium.com/uvc-partners-news/the-european-quantum-computing-startup-landscape-a115ffe84ad8

El ecosistema en España

El "eQosistema" nacional en comunicaciones cuánticas

Industria

indra, hispasat, gmv, Telefónica, cellnex, ThalesAlenia Space, oesia, ALTER TECHNOLOGY

Entidades Nacionales

GOBIERNO DE ESPAÑA – MINISTERIO DE CIENCIA E INNOVACIÓN; CDTI; FECYT

GOBIERNO DE ESPAÑA – MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO

GOBIERNO DE ESPAÑA – MINISTERIO DE DEFENSA; CCN centro criptológico nacional

GOBIERNO DE ESPAÑA – MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

Centros de Investigación

ICFO, CSIC, i2cat, CTTC, Barcelona Supercomputing Center, redimadrid, INTA, imdea nanociencia software, Red IRIS, Instituto de Astrofísica de Canarias

Universidades

Politécnica Madrid, UPV EHU, Universidad de Sevilla, UPC, Universidade Vigo, Universidad Complutense Madrid

PyMES

QUSIDE, Entanglement Partners, VLC Photonics, SATELIOT, DAS Photonics, LUXQUANTA

Otros

Ametic, BBVA, bqb

www.linkedin.com/in/**pvelando**/