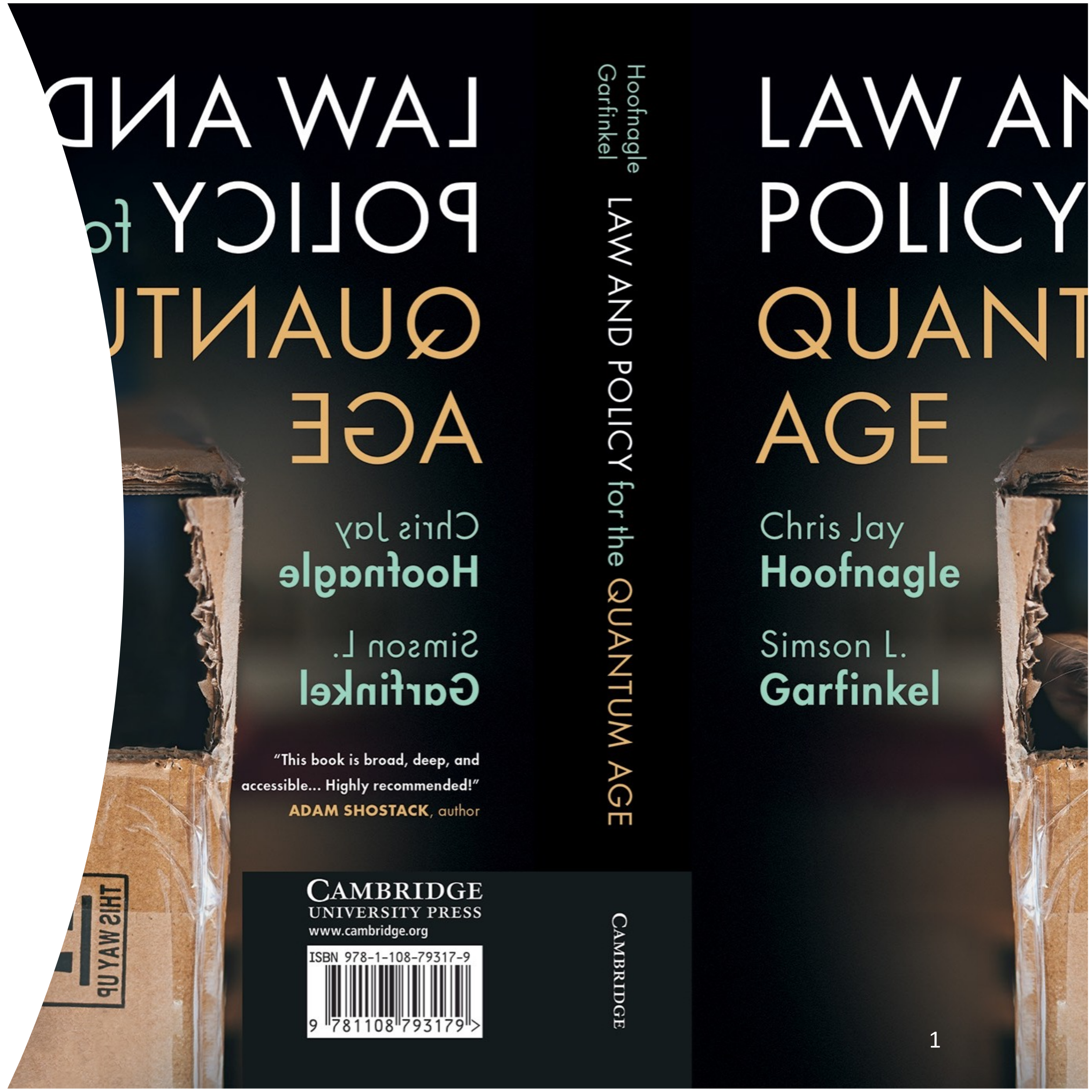
Quantum Technologies: Legal and Policy Issues

Chris Hoofnagle

UC Berkeley

for Professor Wenting Zheng's Cryptosystems



Background & roadmap

Joint work with Simson Garfinkel

- IN PRODUCTION! *Law and Policy for the Quantum Age* (Cambridge University Press 2021)

Quantum technologies (QT) use quantum effects to provide utility---

- Metrology & sensing
- Computing
- Communications

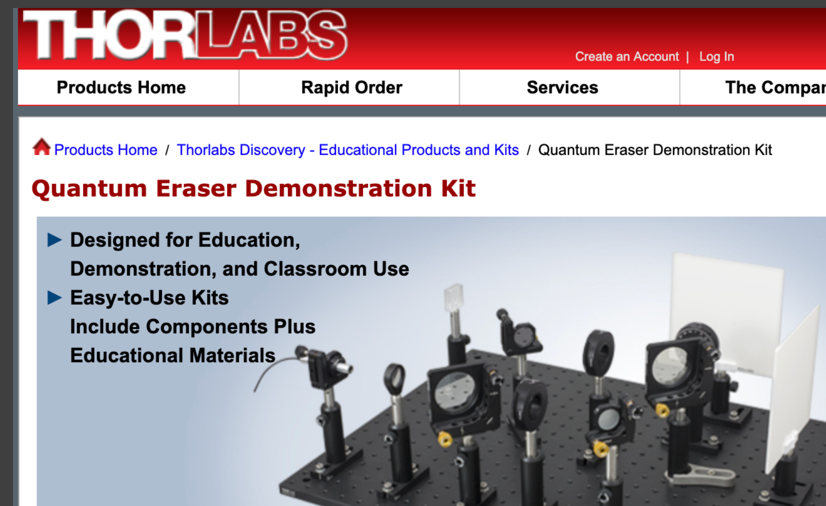
Scenarios

Policy issues

- The problem of technology “novelty” framing

Quantum Technology: why now?

- China & EU investment
  - Leapfrog U.S.
    - Countermeasures for Signals Intelligence (SIGINT)
    - Next-gen tech industry
- Electronic warfare / Measurement & Signature Intelligence (MASINT)
- Tech fundamentals
  - Even commercial products can produce, control, measure quantum-level phenomena
  - Some QTs do not require supercooling



QT: why now?

Corporations—about 200 public & private with significant QT (Pitchbook, Cruchbase)

- Fear that QTs are "winner take all"
- Major challenges
  - Export controls & secrecy
  - Path to profit
  - Spotting quantum fluff
  - Grooming trained workforce

U.S. Govt

- Strong industrial policy approach promising billions of investment through the National Labs (thus basic & applied research, secrecy) + export controls

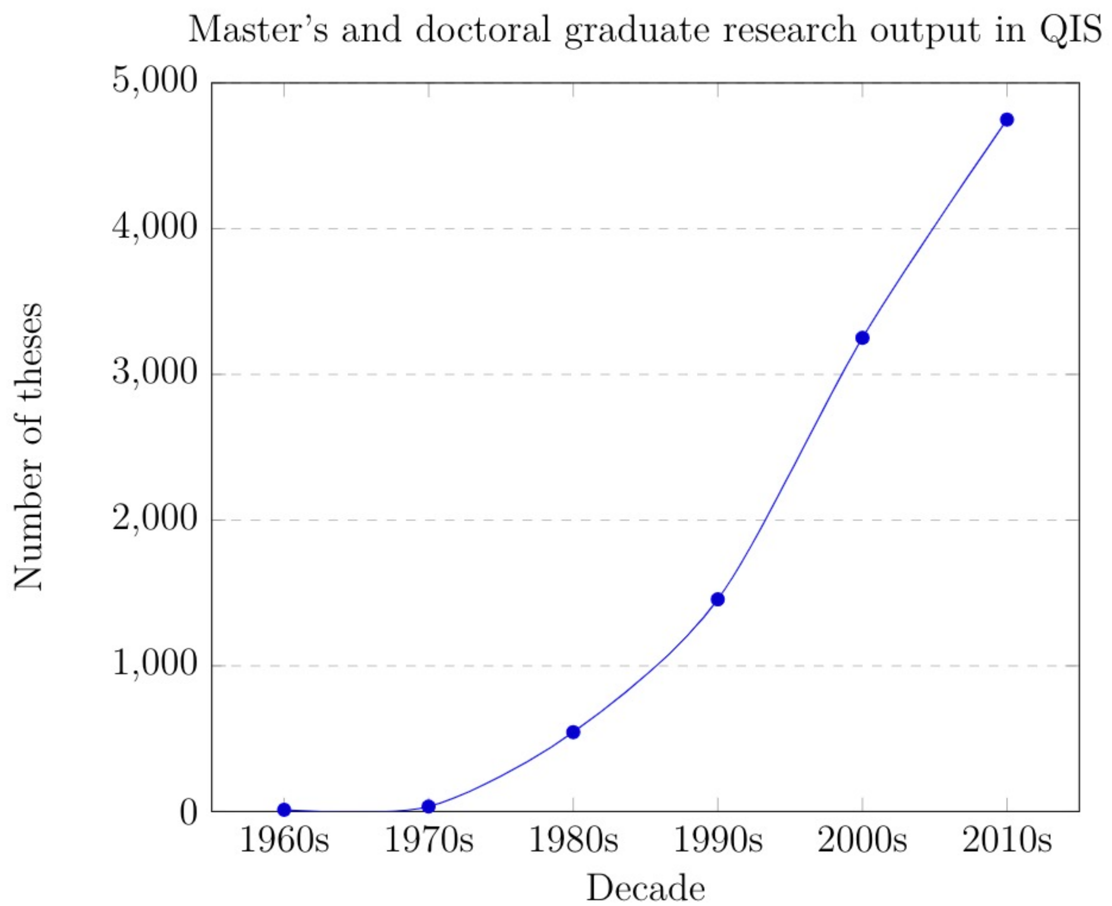
- Nations are funding quantum technology research
- This is a lower-bound estimate of the number of published papers in quantum technology funded by different nation states.

Table 8.1: Support for publications on quantum technologies

Nation	Estimated Number of Papers
China	8 006
US	6 071
European Union including national support	5 819
EU alone	2 520
Japan	1 491
Canada	1 425
UK	894
Germany	785
Nongovernmental Organizations (Foundations)	618
Australia	598
Brazil	518
Spain	455
Russia	383
France	280
Austria	253
Korea	249
Papers with no data	4 641
Total	35 006

- People power really matters.

- The last decades have seen strong growth in QIS training



- The U.S., U.K., China, and Canada are training the QIS workforce

Table 8.11: Institutions more than 100 dissertations and theses were published on QIS

Institution Name	Number of Works
Massachusetts Institute of Technology	253
University of California, Berkeley	225
University of Oxford	198
University of Illinois at Urbana-Champaign	176
Purdue University	165
University of California, Santa Barbara	159
Princeton University	156
University of Maryland, College Park	156
Harvard University	148
University of Cambridge	144
University of Toronto	138
Stanford University	121
Northwestern University	118
University of Michigan	117
Cornell University	111
California Institute of Technology	110
Tsinghua University	110
Imperial College London	109
The University of Texas at Austin	108
University of Rochester	105
University of Colorado at Boulder	103
The University of Wisconsin - Madison	101

Quantum sensing

Oldest category of QT
- Magnetic, gravimetric, photonics

Precursor for quantum computing

We argue that quantum sensing is the "killer app" of QTs
- Not just improvements; **new capabilities**
- Stealthy sensing
- Medical
- EW countermeasures, PNT
- Single-quanta radio
- Quantum radar/sonar
- Ghost imaging
- Mining

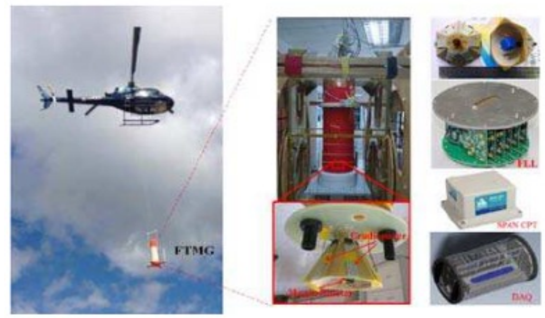
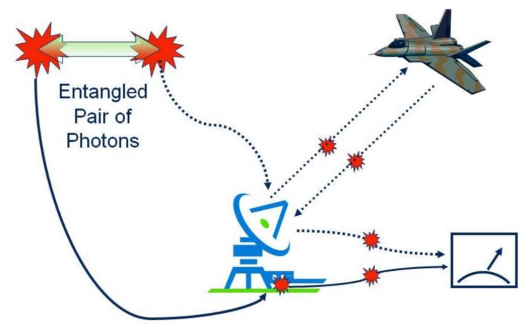
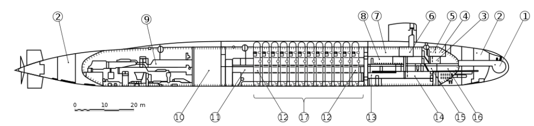


Figure1: schematic diagram of the airborne Superconducting FTMG system.





Quantum computing

State of the science is still in research device status

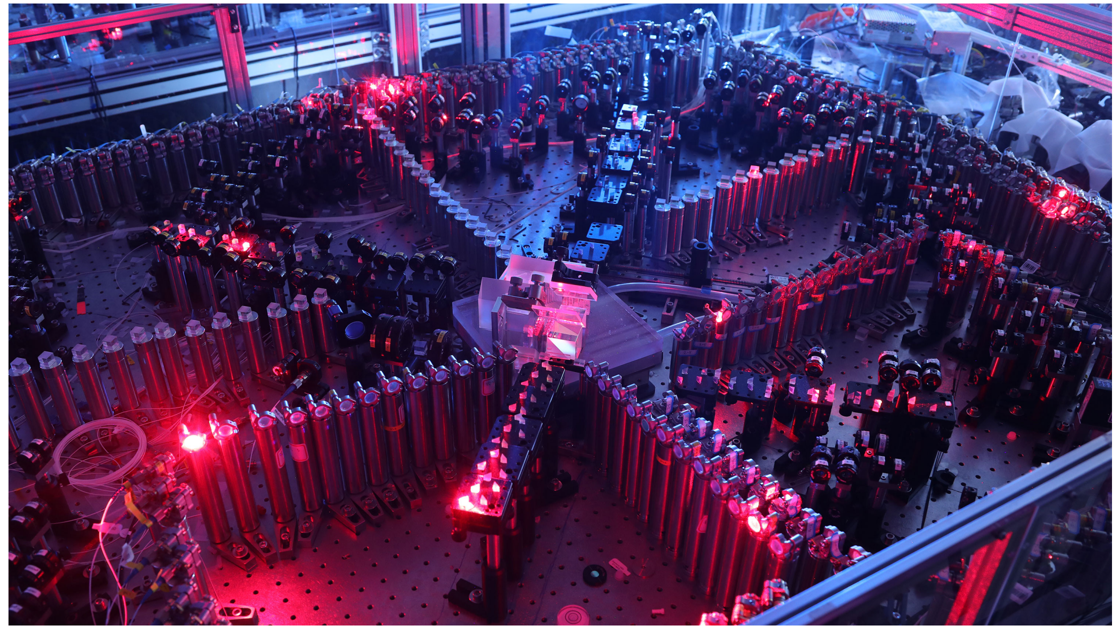
QCs **do not** consider all possible solutions!

Instead, QCs come to solutions faster by taking fewer steps

- Some speedups are exponential (Shor factoring)
- Some are quadratic (Grover search)
- Cryptanalysis a long way off

Simulation in chemistry, materials science is the "killer app"

- Feynman vision for QC
- Winner take all
- Promising for society
- Less legible, therefore not hyped



China's "father of quantum," Jian-Wei Pan recently demonstrated quantum *advantage* with the Jiuzhang device. Jiuzhang is a complex (25 source) interferometer, showing the link between quantum *sensing* and quantum *computing*

Contrary to all the news…QCs will not be encryption killers

Attackers need to have the data, know the algo, have time to make the attack + large QC. ∴ total confidentiality collapse is impossible.

Not an economically productive use of QCs & can be regulated

Govs will focus on *key value*: certificates

Only some encryption is vulnerable

There are numerous countermeasures:

Data at rest: AES/SHA-256

Password compromise: change your passwords

Post-quantum approaches

TABLE 4.1 Literature-Reported Estimates of Quantum Resilience for Current Cryptosystems, under Various Assumptions of Error Rates and Error-Correcting Codes

Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required[a]	Time Required to Break System[b]	Quantum-Resilient Replacement Strategies
AES-GCM [5]	Symmetric encryption	128 192 256	128 192 256	Grover's algorithm	2,953 4,449 6,681	4.61×10^6 1.68×10^7 3.36×10^7	2.61×10^{12} yrs 1.97×10^{22} yrs 2.29×10^{32} yrs	
RSA [6]	Asymmetric encryption	1024 2048 4096	80 112 128	Shor's algorithm	2,290 4,338 8,434	2.56×10^6 6.2×10^6 1.47×10^7	3.58 hours 28.63 hours 229 hours	Move to NIST-selected PQC algorithm when available
ECC Discrete-log problem[c] [7,8]	Asymmetric encryption	256 386 512	128 192 256	Shor's algorithm	2,330 3,484 4,719	3.21×10^6 5.01×10^6 7.81×10^6	10.5 hours 37.67 hours 95 hours	Move to NIST-selected PQC algorithm when available
SHA256 [9]	Bitcoin mining	N/A	72	Grover's Algorithm	2,403	2.23×10^6	1.8×10^4 years	
PBKDF 2 with 10,000 iterations[d]	Password hashing	N/A	66	Grover's algorithm	2,403	2.23×10^6	2.3×10^7 years	Move away from password-based authentication

✔ ✔ ?

National Academies 2019

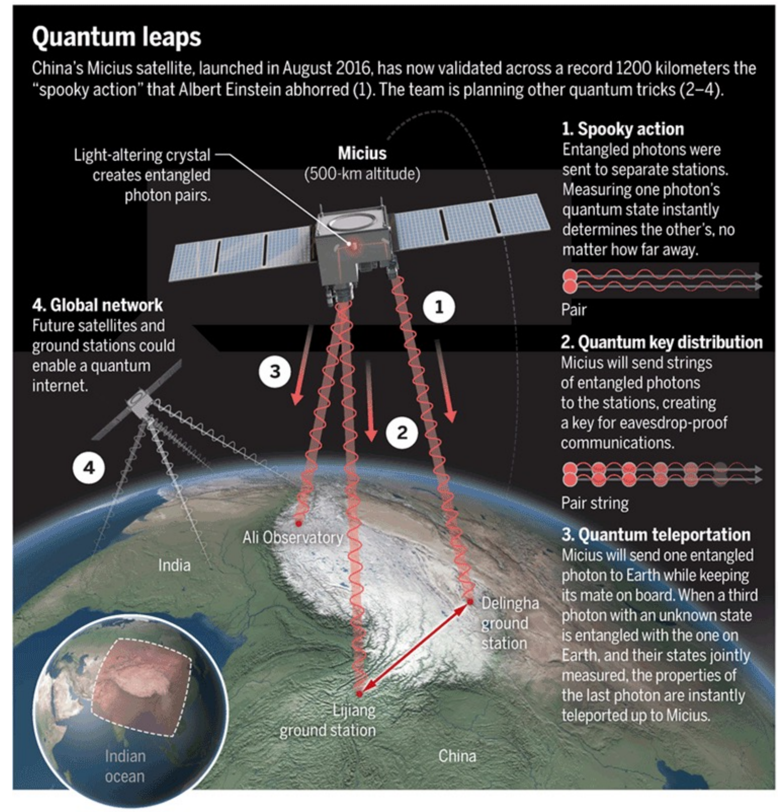
Quantum communications

Quantum-enhanced classical encryption

- Uses quantum effects to enhance existing systems
  - Quantum random number generation (QRNG)
  - Quantum key distribution (QKD)
    - Consequential development---Jian-Wei Pan's satellite QKD (now over 150 users, 4,600 km network)

Quantum networking/internet

- Uses quantum effects to communicate
- Truly end-to-end (no network "trust"):
  - Detect eavesdroppers
  - **Strategic surprise: Deny adversaries access to metadata**
- Potential to connect small quantum computers

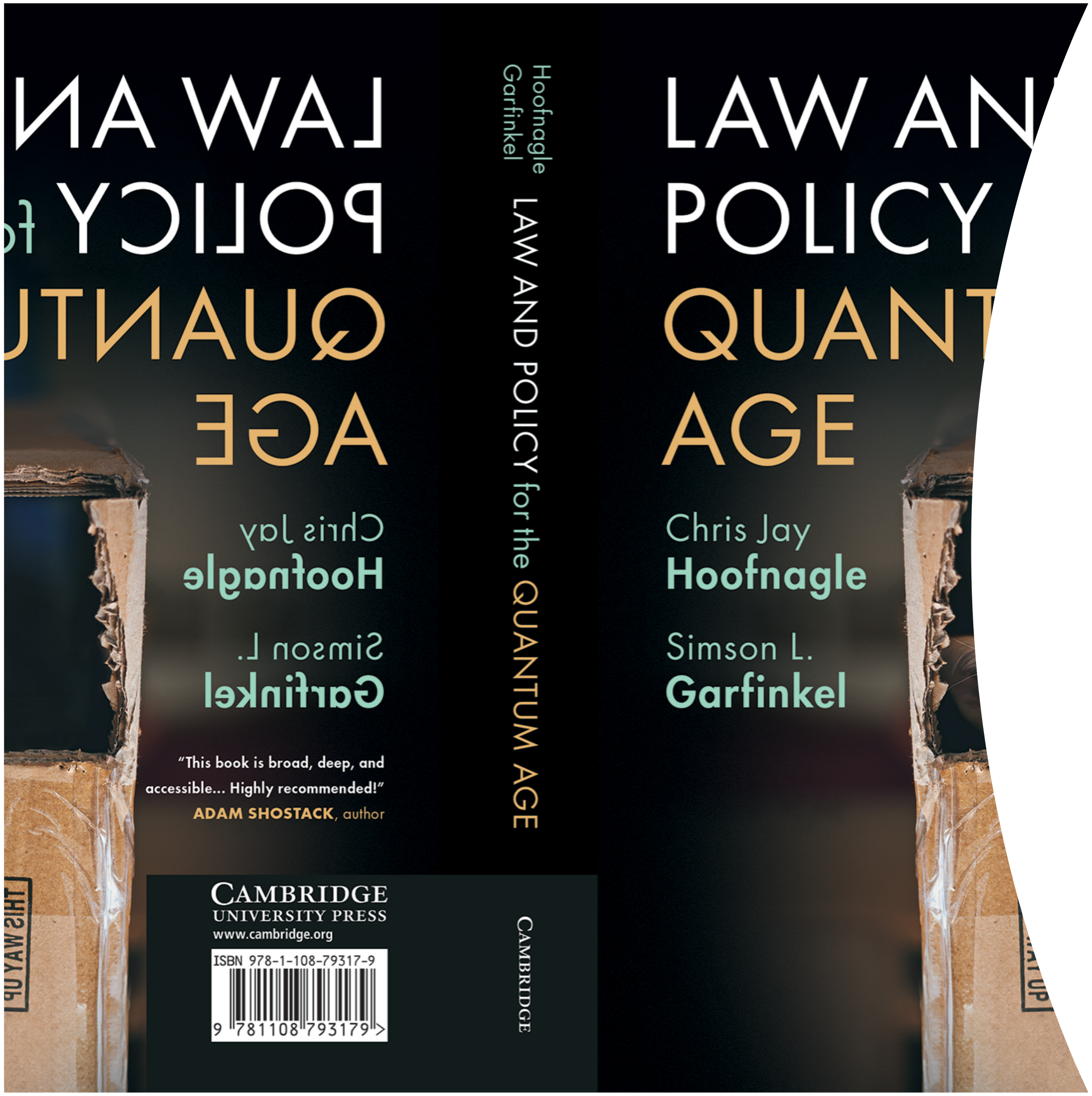


The state of the science published research in Q computing & in Q communication come from China---Jian-Wei Pan & Chao-Yang Lu from USTC-Hefei

Policy scenarios

- Government superior and dominant scenario
  - Could be China (ahead in 2 categories of state-of-the-science innovation)
  - Example of strategic surprise
    - Gov't has Q encryption but also cryptanalysis powers
      - Issue of "key value"
- Public/private utopia scenario: most likely scenario for sensing
  - Example of strategic surprise: authoritarian high modernism (Scott, Seeing Like a State)
    - E.g. smart cities, planned economies
- Public/private, East/West bloc scenario
- Quantum winter: This is a likely scenario for computing

Policy Issues



Thank you ☺

https://the-quantum-age.com/