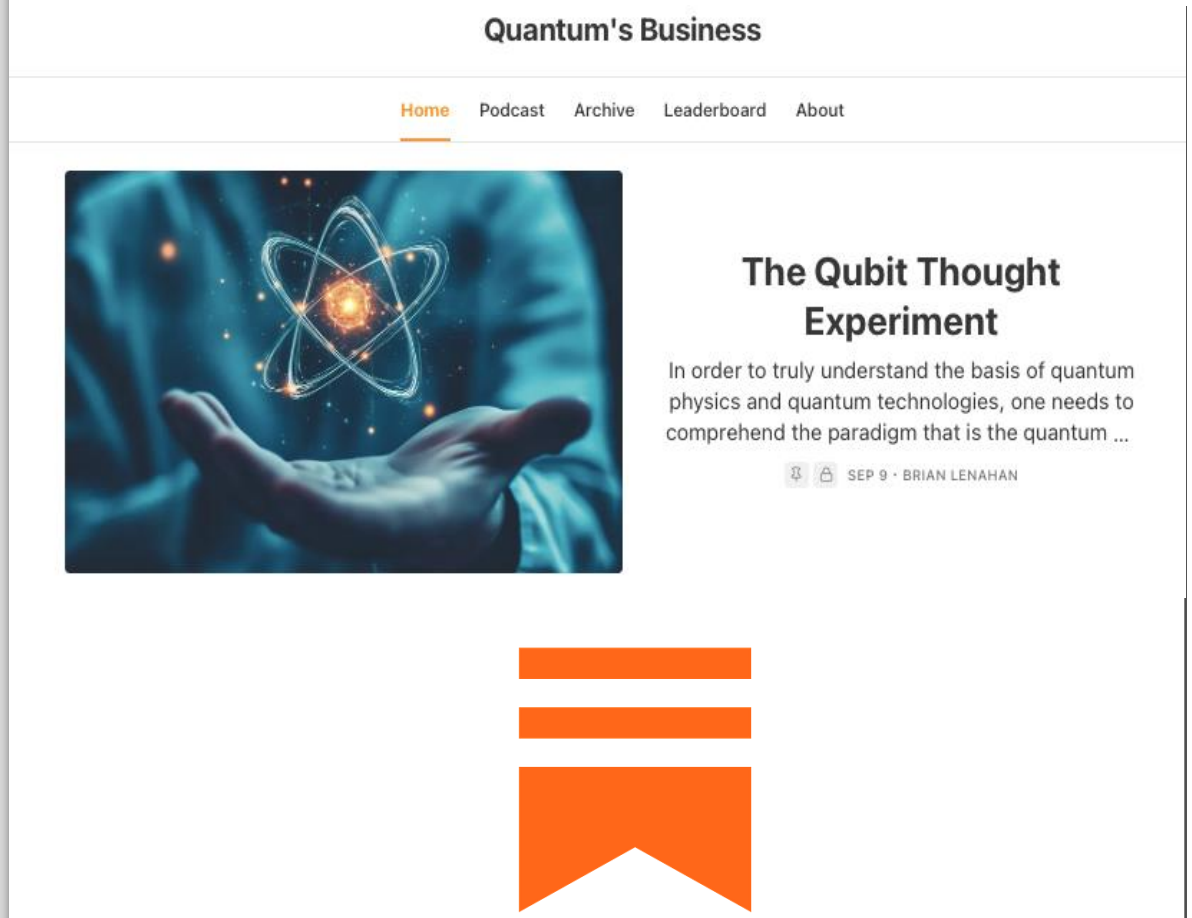
Preparing for Q-Day - The Quantum Threat

Session 3C

Brian Lenahan, Chair - Quantum Strategy Institute
Gregory Carpenter, Chief Security Officer - KnowledgeBridge International



Quantum Strategy Institute

QSI's Report on Cryptography

Taking a Data-Driven Approach to the Quantum Computing Threat

Danika Hannon
Deputy Head, International Quantum Strategy Day Chair
Quantum Strategy Institute

Agenda

- Brief introduction to quantum computing
- Quantum cryptography
- Timelines for Q-Day
- Real-life examples
- Strategies in preparing your organization for Q-Day
- Real-life examples
- Wrap-up

What is Quantum Computing?

1

Overview of quantum mechanics principles (superposition, entanglement)

2

Difference between classical and quantum computing

3

Current state of quantum computing development

Classical Computing

Based on bits, which are the smallest units of information and can be either 0 or 1.

Computers process information using logical operations and circuits that manipulate these bits in a predictable way.

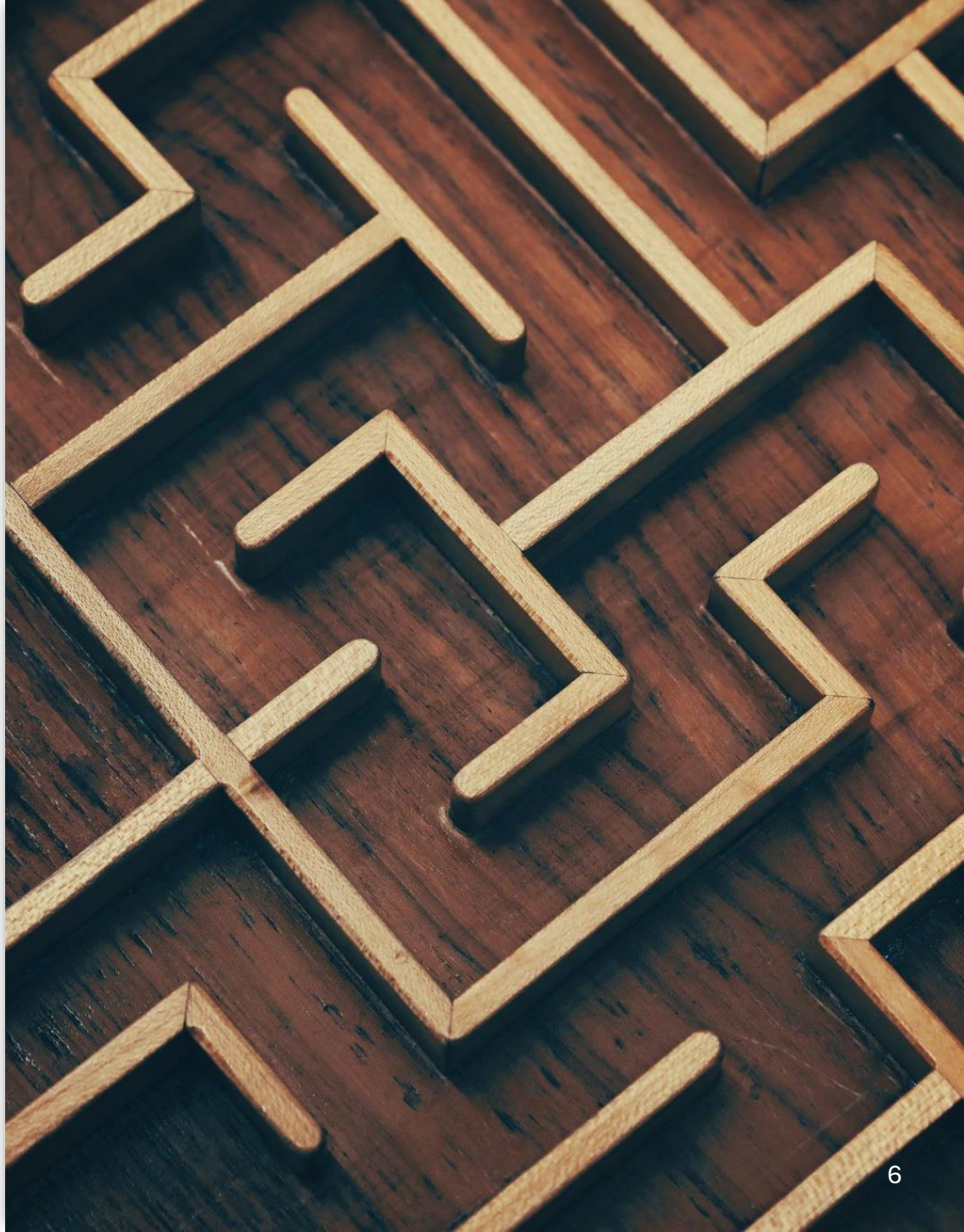
The foundation of classical computing follows the principles of classical physics, meaning operations are **deterministic**—given the same input, a classical computer will always produce the same output.

This model underlies everything from **simple calculators to supercomputers**, using **binary logic and transistors** to perform calculations.

Linear approach to solving problems

Quantum Computing

- Solving The MAZE
- allows quantum computers to perform many calculations simultaneously, drastically increasing their potential speed for certain problems.
- Based on quantum bits or **qubits**
- Can exist in a superposition of **both 0 and 1 at the same time**.
- Relies on **entanglement**, where qubits become correlated in ways that classical bits cannot, allowing for faster information processing and communication.
- Principles come from **quantum mechanics**



Quantum Computing Hardware Modalities

- Superconducting
- Ion Trap
- Photonics
- Neutral Atom
- Nitrogen Vacancy Diamond
- Topological
- WINNER?

Quantum Computing and Cybersecurity

- How quantum computers break classical encryption
  - **On a classical computer**, factoring a 2048-bit number takes billions of years.
  - **On a sufficiently large quantum computer**, Shor's algorithm could factor a 2048-bit RSA key **in hours or minutes**, rendering RSA and similar encryption methods obsolete.
- Risk of **"harvest now, decrypt later,"** and ensure new software development projects follow quantum-ready design principles.
- **RSA, Diffie-Hellman, and ECC encryption** would be vulnerable once large-scale quantum computers become available.
- Threats to RSA, ECC, and other cryptographic protocols – GREG

Quantum-Safe Cryptography

- Introduction to post-quantum cryptography (PQC)
- Designing encryption methods that can resist attacks from quantum computers.
- Today's encryption relies on mathematical problems that regular computers struggle to solve, like factoring large numbers. However, quantum computers could solve these problems quickly, breaking current security systems.
- PQC develops new encryption methods based on problems that even quantum computers can't solve easily, ensuring that sensitive data remains safe in the future.
- Introduction to quantum-key distribution (QKD)
- a way to **securely share encryption keys**
- relies on the fact that measuring a quantum system changes it, so if an eavesdropper tries to intercept the key, their presence is immediately detected.
- ensures that only the intended recipient can receive the key safely.
- Once the key is shared securely, it can be used with traditional encryption methods to protect communication.

Timeline for Quantum Advancements and Potential Threats

- NATO
- US Govt
- China
- Modalities

Q-Day: Cloud Security Alliance says **April 14, 2030**

- estimate of when a quantum computer will be able to break present-day cybersecurity infrastructure.

Public Sector Quantum Use Cases - 1

1. **Cybersecurity and Data Protection**
   - *Challenge*: Public sector systems, such as government databases and critical infrastructure, face increasing cyber threats, including sophisticated encryption-breaking attempts.
   - *Quantum Solution*: Quantum cryptography (e.g., quantum key distribution) could provide unbreakable encryption, ensuring secure communication and safeguarding sensitive data like citizen records, national security information, and healthcare data.
2. **Healthcare Optimization**
   - *Challenge*: Managing large-scale public health systems, optimizing drug discovery, and personalizing treatments are resource-intensive and complex.
   - *Quantum Solution*: Quantum computing could simulate molecular interactions at an unprecedented level, accelerating drug development, optimizing hospital resource allocation, and improving disease modeling for pandemics.
3. **Climate Change and Environmental Management**
   - *Challenge*: Governments struggle to model climate systems accurately and optimize renewable energy grids due to computational limitations.
   - *Quantum Solution*: Quantum algorithms could enhance climate modeling, improve weather forecasting, and optimize energy distribution systems, aiding in disaster preparedness and sustainable resource management.
4. **Transportation and Logistics**
   - *Challenge*: Public transportation systems and supply chains face inefficiencies in routing, traffic management, and resource allocation.
   - *Quantum Solution*: Quantum optimization algorithms could solve complex logistical problems, reducing congestion, improving public transit efficiency, and optimizing disaster relief distribution.
5. **National Defense and Intelligence**
   - *Challenge*: Analyzing vast amounts of intelligence data and detecting threats in real-time are critical yet computationally demanding tasks.
   - *Quantum Solution*: Quantum computing could enhance pattern recognition, decrypt intercepted communications faster (with quantum-resistant countermeasures in place), and improve radar and sensor technologies through quantum sensing.

Public Sector Quantum Use Cases - 2

1. **Public Finance and Economic Modeling**
   - *Challenge*: Economic forecasting and managing public budgets involve complex variables and uncertainties.
   - *Quantum Solution*: Quantum computers could run advanced simulations to predict economic trends, optimize tax policies, and detect financial fraud more effectively.
2. **Criminal Justice and Law Enforcement**
   - *Challenge*: Processing large datasets for crime prediction, forensic analysis, and case backlog reduction is time-consuming.
   - *Quantum Solution*: Quantum algorithms could accelerate DNA analysis, improve predictive policing models, and optimize resource allocation for law enforcement agencies.
3. **Education and Workforce Development**
   - *Challenge*: Personalizing education and reskilling programs for large populations is difficult with current technology.
   - *Quantum Solution*: Quantum computing could analyze vast datasets to tailor educational curricula, predict workforce trends, and optimize training programs for public sector employees.
4. **Disaster Response and Resilience**
   - *Challenge*: Coordinating rapid, effective responses to natural disasters or crises is hindered by limited predictive and logistical capabilities.
   - *Quantum Solution*: Quantum-enhanced simulations and sensing could improve early warning systems, optimize evacuation routes, and enhance real-time decision-making during emergencies.
5. **Public Administration and Policy Development**
   - *Challenge*: Crafting evidence-based policies requires analyzing complex, multifaceted data across demographics, economics, and social factors.
   - *Quantum Solution*: Quantum technology could process and model this data more efficiently, enabling more accurate policy simulations and impact assessments.

Privacy Implications and Public Sector Challenges (Greg)

- Risks to government data privacy and classified information
- Impact on secure communications, digital signatures, and authentication
- Case studies of quantum threats to national security

Strategies for Readiness and Next Steps

Strengthen National Security Applications

Broaden the focus to include the use of quantum technologies in intelligence, defense and threat analysis to enhance overall national security capabilities.

Example GPS vs Quantum sensor navigation

Secure communication via quantum communication

Quantum firewalls – multiple approaches

AUKUS Pillar 2

- Pillar 2 technologies include:
  - undersea capabilities;
  - **quantum technologies**;
  - artificial intelligence and autonomy;
  - advanced cyber;
  - hypersonic and counter-hypersonic capabilities;
  - and electronic warfare.
- The aim of Pillar 2 - leverage the unique strengths of the AUKUS countries' respective innovation bases, to create larger markets for U.S. and allied defense firms and to reduce redundant research and development.
- Although the United States possesses the largest and most competitive technology sector in the world, the United Kingdom's and Australia's technology sectors remain extremely vibrant, with many complementary innovation ecosystems.
- https://www.nationaldefensemagazine.org/articles/2025/2/28/emerging-technology-horizons-accelerate-aukus-pillar-2-to-lead-in-emerging-technologies

Adopt Quantum-Safe Security Standards

Begin	Begin transitioning toward post-quantum cryptography by integrating quantum-resistant algorithms and hybrid infrastructures.
Establish	Establish data protection policies that treat sensitive information as at risk of “harvest now, decrypt later,”
Ensure	Ensure new software development projects follow quantum-ready design principles.
Establish	Establish relationships with credible vendors
Get ahead	Get ahead of future compliance laws

Strategies for Readiness and Next Steps

- Implementing quantum-safe security measures
  - % of Govt preparing – US vs Canada;
  - QSI Reports
  - Substacks
  - Canadian Centre for Cybersecurity
  - Credible vendors
- Building awareness and training within government agencies - GREG
- Collaboration with industry and academia for quantum readiness;
  - UBC resources – QMI
  - Regional Quantum Initiative in British Columbia
  - UBC and D-Wave to Host The Adiabatic Quantum Computing 2025 Conference in Vancouver

Quantum's Business

Home Podcast Archive Leaderboard About

The Qubit Thought Experiment

In order to truly understand the basis of quantum physics and quantum technologies, one needs to comprehend the paradigm that is the quantum ...

SEP 9 · BRIAN LENAHAN

Quantum Strategy Institute

QSI's Report on Cryptography

Taking a Data-Driven Approach to the Quantum Computing Threat

Danika Hannon
Deputy Head, International Quantum Strategy Day Chair
Quantum Strategy Institute