Government
Digital & Data

Post-Quantum Cryptography

Selling magic to accountants

Martin Bowyer
Central Digital & Data Office, UK Government

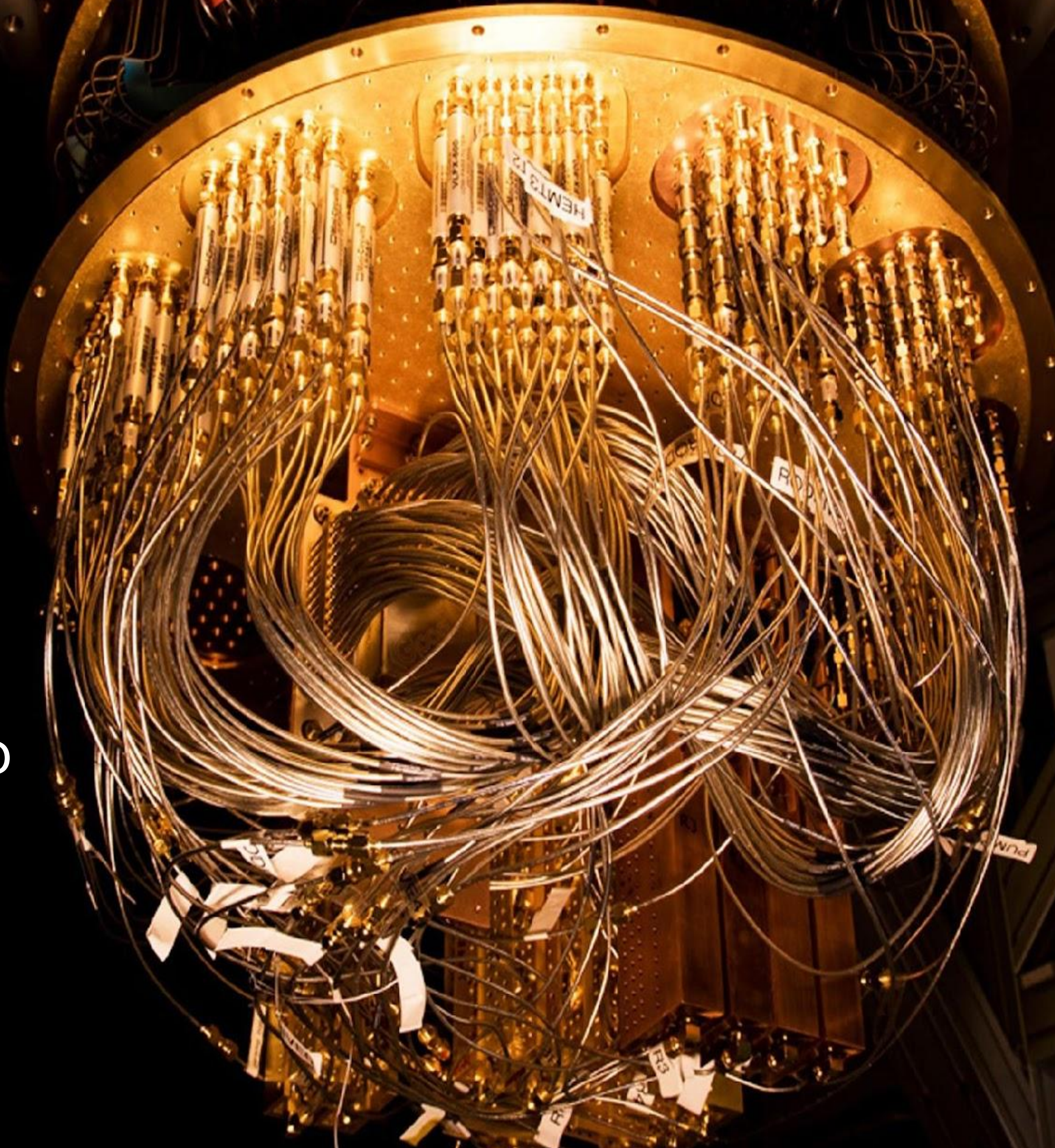
December 2024

How can we help Government decision makers to understand the threat posed by quantum computing to classical cryptography and therefore balance the priority, costs and resources required to manage and mitigate the risk this presents to delivering the organisation’s services and protecting the data for which they are responsible, given the scale of the task, the likely timescales involved and all the other risks and demands they have to manage?

Why is starting the PQC Journey like selling magic to accountants?

Belief is important

- Quantum computing sounds like magic
- Magic shakes our predictable world
- Fire alarms and cyber risk
- So how do we get people to instinctively believe in quantum computing and the threat?

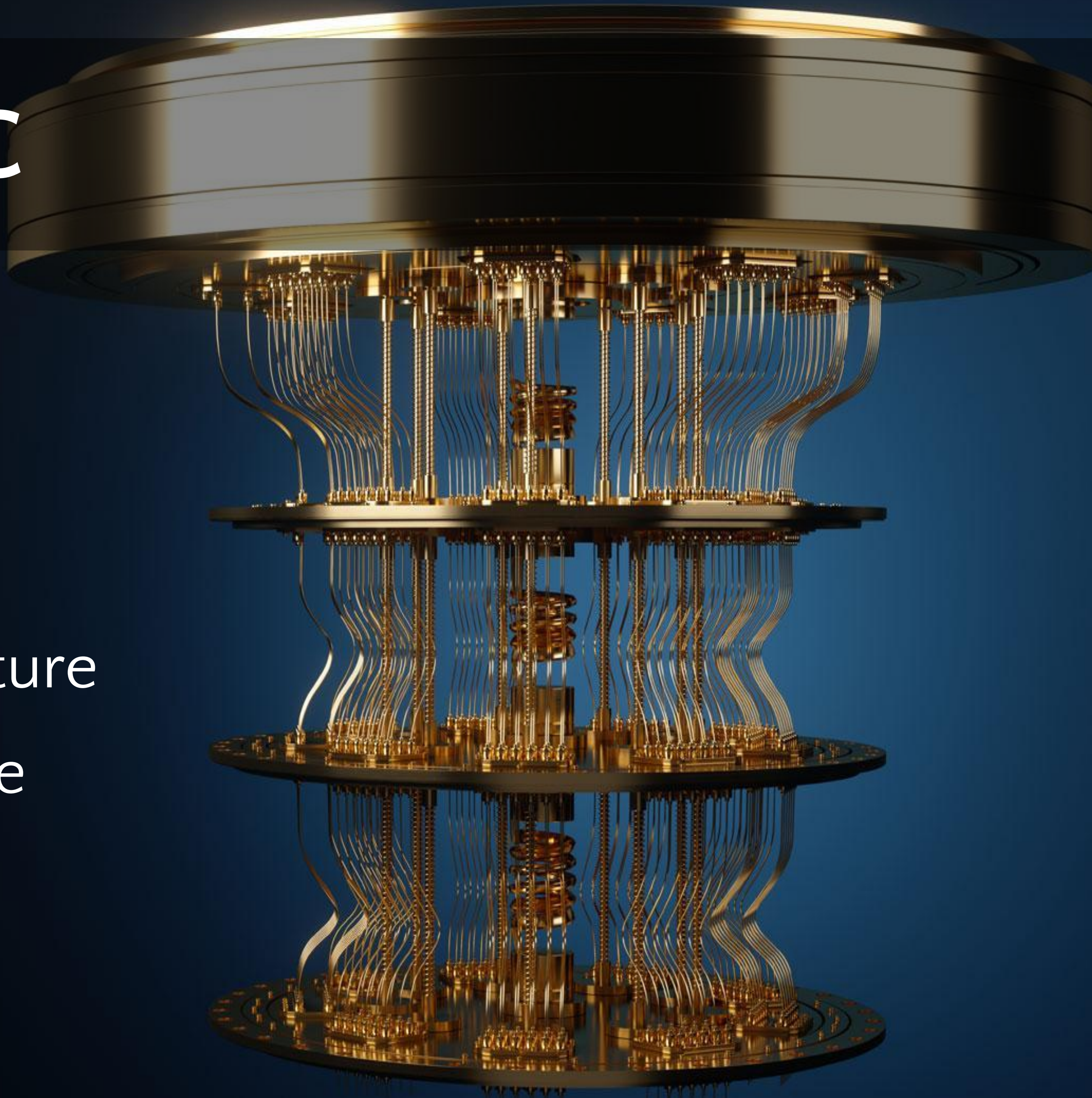


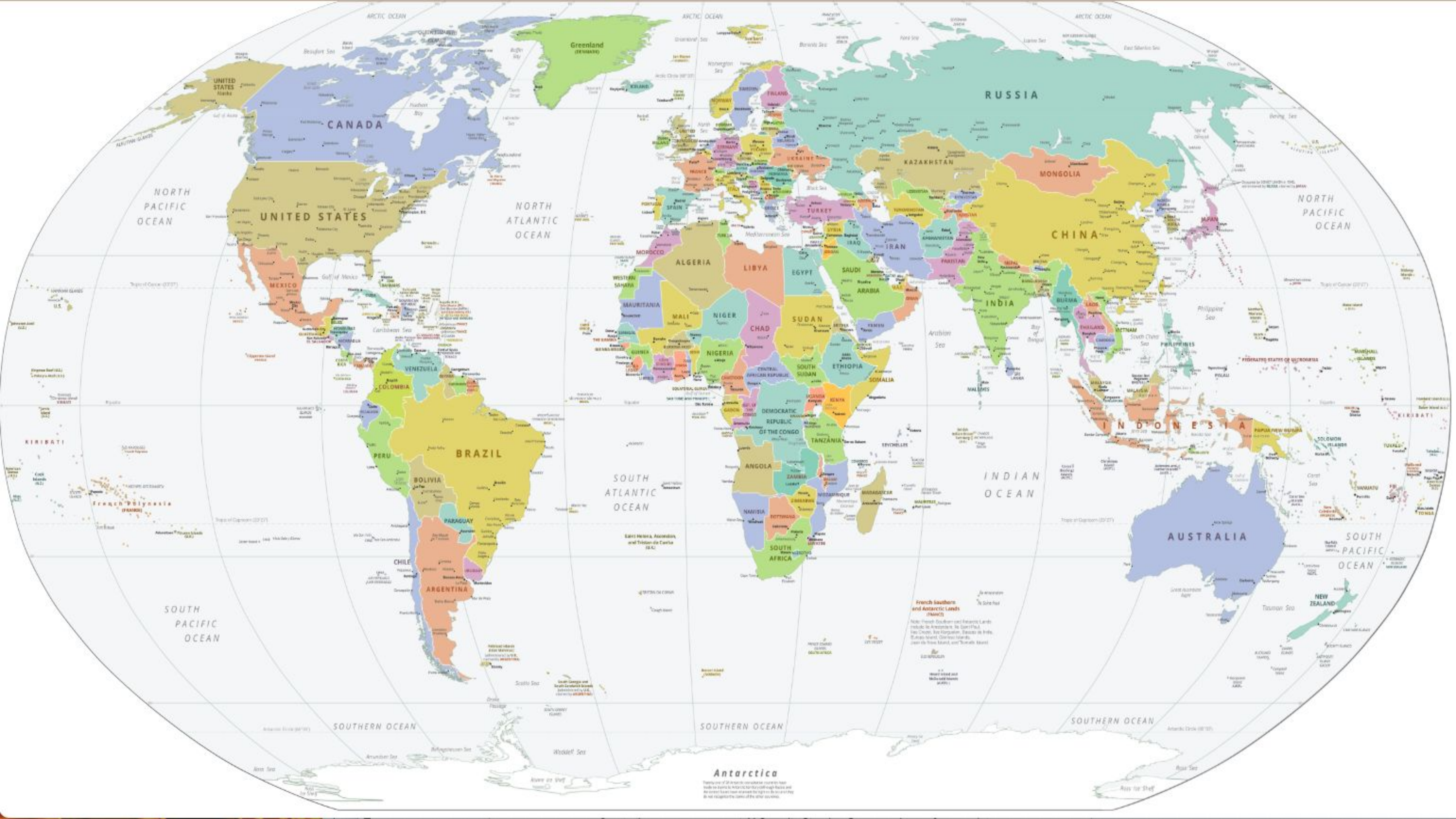
Quantum magic

Demystifying PQC

- Comfort in data and facts
- Bounding the problem
- Showing a credible plan
- Paint the picture of the future

  …and the alternative future




ARCTIC OCEAN
ARCTIC OCEAN
ARCTIC OCEAN
Greenland
(DENMARK)
Beaufort Sea
Greenland Sea
Barents Sea
Norwegian Sea
Kara Sea
Laptev Sea
East Siberian Sea
Hudson Bay
Bering Sea
UNITED STATES
Alaska
CANADA
RUSSIA
ICELAND
FINLAND
SWEDEN
NORWAY
North Sea
UNITED KINGDOM
IRELAND
GERMANY
POLAND
BELARUS
UKRAINE
FRANCE
SPAIN
PORTUGAL
ITALY
GREECE
Black Sea
KAZAKHSTAN
MONGOLIA
NORTH PACIFIC OCEAN
NORTH PACIFIC OCEAN
UNITED STATES
NORTH ATLANTIC OCEAN
TURKEY
Mediterranean Sea
SYRIA
IRAQ
IRAN
AFGHANISTAN
PAKISTAN
TURKMENISTAN
UZBEKISTAN
CHINA
JAPAN
NORTH KOREA
SOUTH KOREA
MOROCCO
ALGERIA
LIBYA
EGYPT
SAUDI ARABIA
OMAN
YEMEN
NEPAL
INDIA
BANGLADESH
BURMA
LAOS
THAILAND
VIETNAM
CAMBODIA
PHILIPPINES
Philippine Sea
South China Sea
Gulf of Mexico
MEXICO
CUBA
Caribbean Sea
WESTERN SAHARA
MAURITANIA
MALI
NIGER
CHAD
SUDAN
ERITREA
DJIBOUTI
ETHIOPIA
SOMALIA
SOUTH SUDAN
NIGERIA
CENTRAL AFRICAN REPUBLIC
CAMEROON
GABON
DEMOCRATIC REPUBLIC OF THE CONGO
UGANDA
KENYA
TANZANIA
ANGOLA
ZAMBIA
MALAWI
MOZAMBIQUE
ZIMBABWE
NAMIBIA
BOTSWANA
SOUTH AFRICA
MADAGASCAR
SEYCHELLES
MAURITIUS
Arabian Sea
Bay of Bengal
SRI LANKA
MALDIVES
MALAYSIA
INDONESIA
PAPUA NEW GUINEA
SOLOMON ISLANDS
FEDERATED STATES OF MICRONESIA
MARSHALL ISLANDS
KIRIBATI
KIRIBATI
NAURU
TUVALU
VANUATU
FIJI
TONGA
SAMOA
PALAU
French Polynesia
(FRANCE)
Hawaiian Islands
U.S.
VENEZUELA
COLOMBIA
ECUADOR
PERU
BRAZIL
BOLIVIA
PARAGUAY
CHILE
ARGENTINA
URUGUAY
COSTA RICA
PANAMA
SOUTH ATLANTIC OCEAN
Saint Helena, Ascension, and Tristan da Cunha
(U.K.)
INDIAN OCEAN
AUSTRALIA
Coral Sea
Tasman Sea
NEW ZEALAND
SOUTH PACIFIC OCEAN
SOUTH PACIFIC OCEAN
Tropic of Cancer (23°27')
Tropic of Capricorn (23°27')
Equator
Arctic Circle (66°33')
Antarctic Circle (66°33')
French Southern and Antarctic Lands
(FRANCE)
Falkland Islands (Islas Malvinas)
South Georgia and South Sandwich Islands
Scotia Sea
Drake Passage
SOUTHERN OCEAN
SOUTHERN OCEAN
SOUTHERN OCEAN
Weddell Sea
Bellingshausen Sea
Amundsen Sea
Ross Sea
Ross Ice Shelf
Ronne Ice Shelf
Antarctica

Many Voices

The International paper…

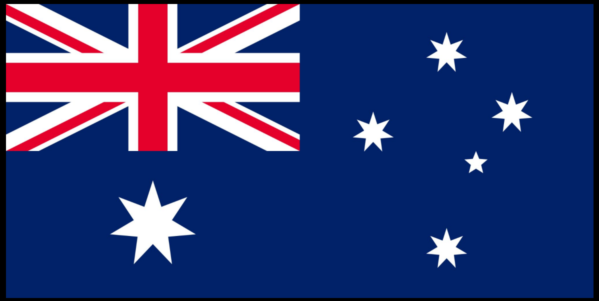
1. Highlights the threat posed by quantum computing and the potential impact on government operations and data security

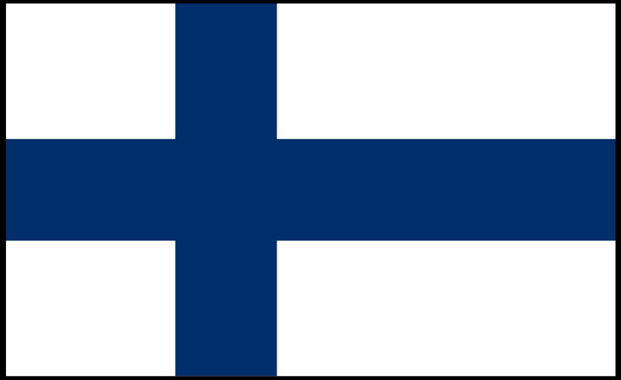
2. Advocates for the active involvement of senior leaders to ensure government adopts a crypto-agile posture

3. Outlines key steps for migrating to PQC cryptography ensuring long-term data protection and resilience

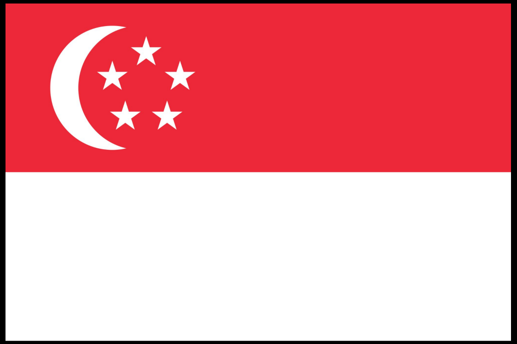
… through a ‘Protecting Government’ lens

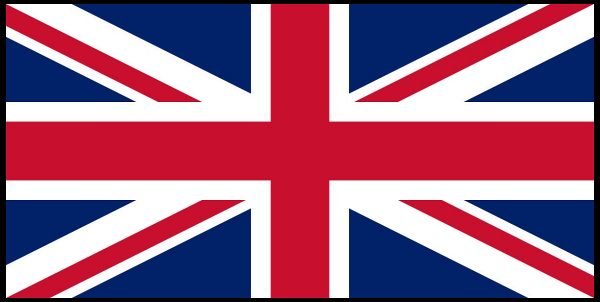
THE WORLD BANK





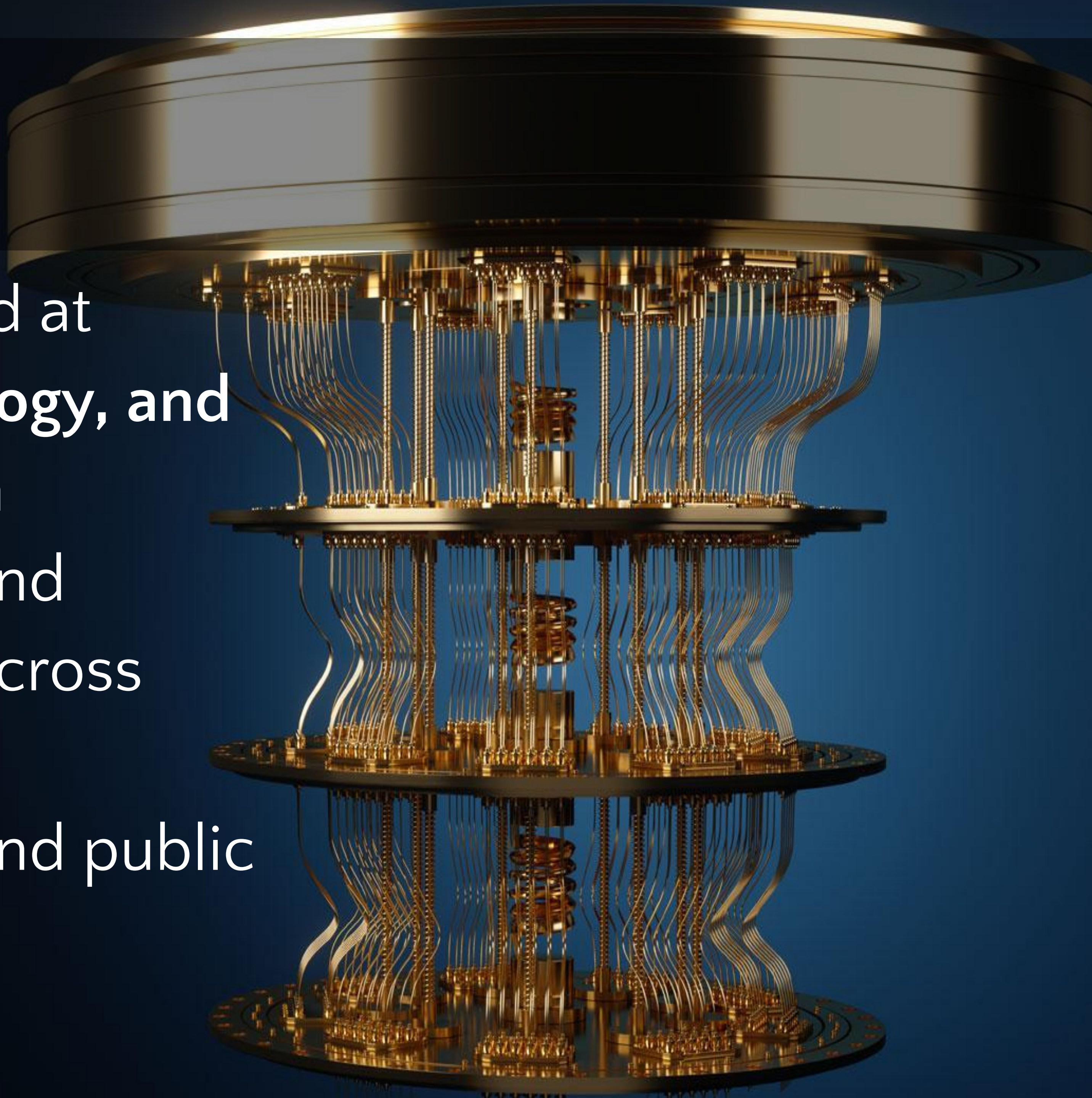
GLOBAL government FORUM





Audience

The paper is primarily aimed at **government policy, technology, and financial leaders** involved in protecting electronic data and securing communications across national security, critical infrastructure, healthcare, and public sector operations.



Key Benefits

- Educate policymakers about an emerging global challenge
- Support advocacy efforts by highlighting critical issues and proposing actionable solutions
- Promote a unified methodology for transitioning government systems to PQC

Overview on a Page

Threat

Current public-key cryptography can't withstand attacks from CRQC threatening data privacy, national security, financial stability, and integrity of digital comms

- *uncertain timescales*
- *supply chain*
- *legacy systems*
- *complex inventory*

Take action now!

- Inventory crypto algorithms
- Allocate adequate funding
- Upgrade crypto infrastructure (change management)
- Ensure ongoing resilience (vulnerability management)

Questions

1. Do you recognise this challenge?
2. How did you move past it?
3. What language works best?
4. How will you keep your policymakers and financial decision makers on board?

Government
Digital & Data

Martin Bowyer
Deputy Director Securing Government Services

martin.bowyer@digital.cabinet-office.gov.uk