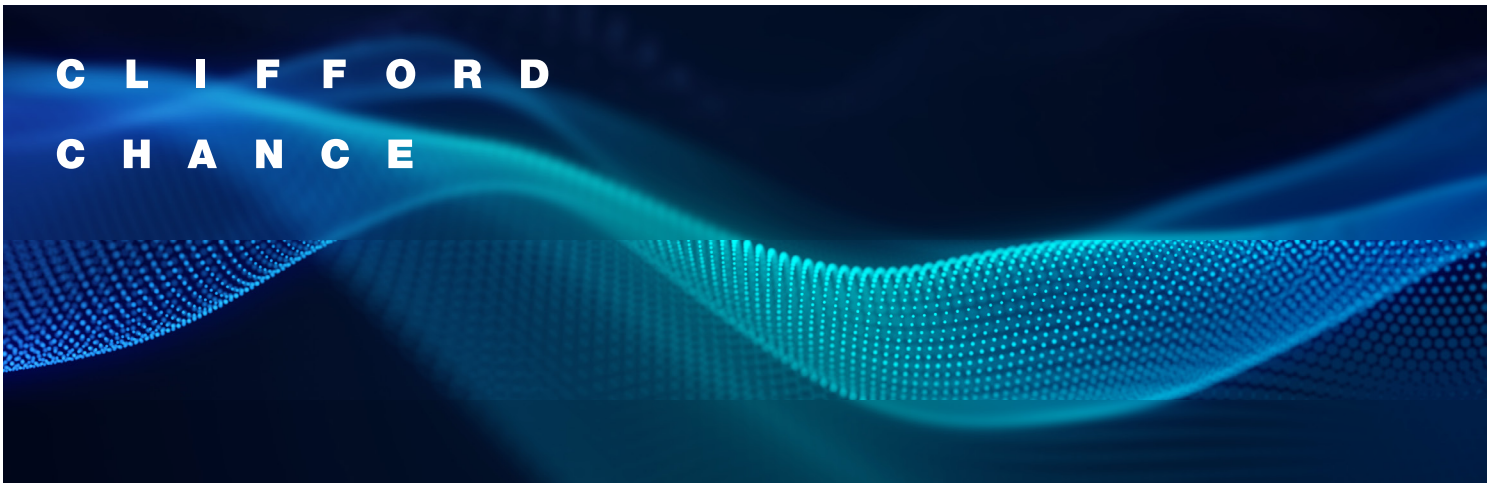

QUANTUM STATE OF PLAY

Quantum technology, although nascent, has the potential to revolutionise computing and to reshape geopolitics as nations race to secure a foothold in this cutting-edge field. But it comes with enormous risks around national security, sovereignty and cybersecurity, as quantum could have the ability to render useless most encryption techniques. In this briefing, we explore the challenges and opportunities that lie ahead together with regulatory and legislative concerns, as a number of jurisdictions impose export controls on (broadly defined) quantum technology.

Why governments are prioritising investment in quantum tech

Policymakers have long understood that new industries need state support to grow and compete. This was the case for cotton textiles, motor cars, electricity, space exploration and the internet. Leadership in quantum technologies is expected to have similarly significant economic, scientific, strategic and national security implications. There has been concern since the 1990s that quantum computing will have the ability to crack the encryption methods that are used to protect our digital data, which will have a huge impact on governments, banks, internet companies – and our individual privacy.

Nation states may be the first to develop quantum computers that are able to break cryptographic systems, enabling them to access the critical national infrastructure of other states including government systems, communications networks, energy, transport and healthcare.

The US National Institute for Standards and Technology (NIST) started work on post-quantum cryptography back in 2016, and that project is continuing. Cryptographers worldwide are working on a new generation of algorithms with quantum computing in mind, seeing the emergence of theoretically "quantum-proof" techniques, sometimes referred to as "post-quantum" cryptography. More recently, China's Institute of Commercial Cryptography Standards has also called for proposals for such algorithms.

Where is the funding coming from?

Building quantum hardware is highly capital-intensive. Public investment, from funding to permissive planning, is essential for any nation that aspires to quantum leadership. Only large companies and research institutions with considerable public support have been able to create the physical infrastructure required to support the development of quantum algorithms and software. Industry collaboration, public-private partnerships and R&D funding are increasing, and the market is predicted to be worth US$10 billion by 2030.

How will businesses use quantum?

The finance, automotive healthcare and industrial sectors appear to be the most interested in the economic potential of quantum computing. In healthcare for example, it could accelerate R&D and in the financial sector it could reduce uncertainty around decision-making.

What are the legal implications?

Data protection: Many of the existing data protection regimes around the world require organisations to take account of the state of the art in adopting measures to protect personal data and, likewise, cybersecurity obligations evolve as the threat landscape changes over time. Regulatory authorities, particularly in the finance sector, are starting to consider express regulation or guidance requiring financial institutions to focus on the quantum transition. For example, in the UK Financial Conduct Authority co-published a whitepaper with the World Economic Forum's Quantum Economy Network advocating for a joined-up approach between regulators and industry, including to address data security risks.

Organisations should take care to keep their information security controls up to date – which is the right approach whether quantum is in the picture or not.

Intellectual property: With technology that is especially difficult for non-technical experts to conceptualise, we anticipate that there will be a drawn-out period of IP disputes and norm-setting as to which companies enjoy the commercial benefits of investments in quantum technology. Numerous patents for quantum technology have already been filed, but it remains to be seen how patents and copyright might apply to protect each layer of the nascent quantum technology stack.

Competition: Quantum resources may one day become a baseline requirement to play in a variety of markets, raising barriers to entry with potentially harmful effects for competition and the interests of consumers. Fortunately, the essential elements of competition and antitrust regulation already in place today stand ready to protect against this.

Operational resilience and risk management: Buying or licensing in cryptographic functionality to support a transition to support a transition to quantum-proof encryption could increase operational risks, attract regulatory scrutiny and/or create new external dependencies. Particularly in the finance sector, legal, IT, infosec and risk management functions should work together closely.

Ethics: Building AI systems using quantum hardware has the potential to significantly expand the power of those systems. With advancements come greater risks to individuals and a heavier burden of responsibility to mitigate ethical challenges, including bias/discrimination, accountability/governance, transparency and explainability. This risk is pronounced in regulated industries such as medical technology and financial markets, where supercharged AI could overwhelm existing protections.

National security, sovereignty, and export and merger control

As countries strive to harness the potential of quantum computing, safeguarding the technology is now a priority. Advancements in quantum promise unprecedented capabilities in secure communications and encryption-breaking, which could alter the balance of power in international relations. With advancements come challenges in regulation and control, as nations adapt their legal frameworks to ensure that technologies developed within their borders do not exacerbate global tensions or destabilise international security environments.

Consequently, nations are implementing stringent export controls to prevent sensitive quantum technologies from falling into the hands of adversaries or unfriendly nations. The UK Government updated its export control regime through changes to The Export Control (Amendment) Regulations 2024, adding new controls on semiconductor technology and quantum technology. The US Treasury issued regulations for the new Outbound Investment Security Program, prohibiting US persons from entering into certain transactions relating, in particular, to the development of quantum computers and the components therein. Meanwhile, the EU's Economic Security Strategy called for expanded screening of outbound investment in quantum technologies. Australia, China, France, Spain and the Netherlands have similarly imposed export restrictions. These measures aim to protect national interests, maintain technological competitiveness, and uphold global stability. However, they also necessitate careful balancing to foster international collaboration and innovation without compromising security. Corporate acquisitions of quantum capability will also increasingly be subject to national security approval.

ANNEX

This Annex sets outs examples of initiatives we are seeing in quantum investment and regulation.

 **Quantum strategy**	• **United States, China, Canada, Japan, The Netherlands, United Kingdom, Germany, South Korea, Australia, France**: National strategies focusing on development and deployment, and technological sovereignty. • **NATO**: Cooperative strategy with industry for a quantum technology ecosystem.
 **Cybersecurity and Post-Quantum Cryptography**	• **World Economic Forum**: Advocated for global regulatory approach to quantum security. • **G7**: Addressed quantum computing risks, recommending financial institutions transition to post-quantum cryptography. • **European Union**: Published recommendations for transitioning to post-quantum cryptography. • **Singapore**: MAS issued circulars to assess quantum computing risks. • **Japan**: Focussed on post-quantum cryptography in the financial sector.
 **Regulatory measures and export controls**	• **United States**: New export controls for quantum computing technologies. • **Australia**: Quantum computers added to the Defence and Strategic Goods List. • **France**: Licensing requirement for exporting quantum technologies outside the EU. • **The Netherlands and the UK**: Restrictions on the export of quantum technology.
 **Industry collaboration, funding, and R&D**	• **United States**: Industry-led initiatives like QED-C, significant government funding for quantum technology, National Quantum Initiative Reauthorization Act. Establishment of quantum computing centres and technological showcases by companies. • **Canada**: Investment in academic research and quantum sensing tech. • **Australia**: Public investments in PsiQuantum, establishment of Quantum Australia. Joint investments between state governments and companies. • **India**: Launched national quantum mission, significant investments in quantum technologies. • **South Korea**: Quantum Initiative, Quantum Frontier Strategy Council. • **Japan**: Developing a 10,000 qubit quantum computer. Collaborations between AIST and IBM. • **Israel**: Opening of the Israeli Quantum Computing Center. • **European Union**: Investment in R&D for quantum chips through Quantum Flagship. • **Germany**: Funding increase for quantum research. • **Switzerland**: Swiss Quantum Call 2024 for research funding. • **The Netherlands**: National Technology Strategy, Quantum Delta NL programme.

CLIFFORD

CHANCE

CONTACTS

James Wong
Lawyer
London
T: +44 207006 3750
E: james.wong@
cliffordchance.com

Oscar Tang
Senior Associate
London
T: +44 207006 3749
E: oscar.tang@
cliffordchance.com

JOB0000051238