Australian National University | NATIONAL SECURITY COLLEGE

Towards the Quad Quantum Network Initiative

Takahiro Tsuchiya

Key points

- Quantum computing and the quantum internet will become fundamental technologies and sources of national power in terms of computational resources and information security.
- The priority for Quad countries should be the development Quantum Processing Units (QPU) that are necessary for Fault-Tolerant Quantum Computing (FTQC) and, over time, a network of quantum computers.
- The challenge for the Quad is to develop a quantum network that covers vaster distances than China's quantum network.

Policy recommendations

- Quad countries must break away from the era of small teams working separately on a country-by-country basis to advance quantum computing research, development, and industrial application.
- Rather than focusing only on Quantum Key Distribution (QKD), Quad countries should prioritise the development of game-changing technology: the QPUs necessary for developing FTQC and quantum networking (quantum internet).
- A Quad Quantum Network Initiative should be launched to promote the unification and harmonisation of international standards for quantum communication technologies, including cryptography and security protocols.

From noisy to fault-tolerant quantum computation

Quantum information science and technology will become a fundamental technology that directly affects national power, especially regarding information security and computational resources. The United States and China are competing over the development of this technology. Other significant countries are focused on developing quantum computers that transmit quantum information on qubits.

The computational power of current quantum computers is limited by noise. These devices are called Noisy Intermediate-Scale Quantum Computers (NISQ). The next milestone will be 'quantum transcendence' – developing NISQ to perform practical quantum chemical computation and quantum learning better than a classical computer. The longer-term goal is Fault-Tolerant Quantum Computation (FTQC). FTQC is essential to finding solutions to simultaneous equations that meet specific conditions, factoring huge numbers, and accelerating calculations in artificial intelligence and data science that deal with vast amounts of data.

To move from NISQ to FTQC, it is necessary to develop Quantum Processing Units (QPUs) that can handle long, time-consuming calculations. The birth of FTQC will make possible analysis of quantum information without digital processing. For example, quantum computers will analyse Magnetic Resonance Imaging (MRI) data, with such studies leading to technologies for disease prevention. It is estimated that the transition from NISQ to FTQC will occur as early as 2029 to 2030 or around 2050 at the latest.

Quantum cryptography and networks

Quantum Key Distribution (QKD) is based on a quantum cryptosystem that uses quantum bits to deliver secret keys for communication between classical computers. The QKD network is a series of trusted nodes that share a secret key and perform quantum-critical delivery. QKD transfers digital bits written in qubits. If an adversary replaces the relay nodes, the QKD network and its digital information may collapse.

China leads the field of QKD in terms of scale, distance, and coverage. In 2016, it was the first country in the world to successfully launch a quantum communication satellite (known as 'Micius' or 'Mozi'). The national quantum secure communication network, which connects Beijing, Shanghai, and Hangzhou (Zhejiang), was completed in 2017. At the very least, China's terrestrial QKD network already extends several thousand kilometres and is scheduled to grow.

China is also making progress in generalising quantum computers and diversifying the applications of QKD. China's QKD network is used for online conferencing systems, data servers, and online big data platforms. China is expected to create an advantageous environment for the domestic diffusion of quantum technology and the development of quantum human resources. As China exports QKD, it is expected to gain international standards and global market share.

Quantum cryptography systems based on QKD technology have reached the commercial stage in other countries. They operate in Europe, the US, and Japan. China, Japan, and Singapore have launched quantum satellites, and the United Kingdom plans to do so in 2024. The Netherlands (Quantum Internet Alliance), Germany (Q Link X), and Spain (OpenQKD) are promoting quantum networking. In Japan, the Tokyo QKD network has been in operation since 2010. It has particular strengths in speed and standardisation, including its use for transmitting biometric data and other protected information.

The US has been working on QKD since 2020, but the US Defence Science Board still assesses that QKD is insufficiently secure to be adopted by the US military. Several networking experiments are also under way in the US, including the Center for Quantum Networks (NSF), the Long Island Quantum Repeater Network, and the Chicago Quantum Network. US research on the Quantum Internet has leaped ahead of other countries.

Towards the quantum internet

As the number of qubits increases, there will be a need for distributed quantum computers. Cloud quantum computation using FTQC, or quantum internet, will be necessary to process such an enormous amount of information and transmit and share it among the countries involved. The quantum internet could harness entanglement and teleportation to transmit quantum information. Unlike the classical internet and QKD networks, the quantum internet will provide quantum information rather than classical information. The fear of classical information being extracted will, therefore, be eliminated.

The Noisy Intermediate-Scale Quantum Internet (NISQI) is expected to be developed shortly and will enable some practical quantum communication. However, there are limitations in communication distance, quality, and bandwidth.

The future high-performance quantum internet will make possible large-scale computation and processing of big data, including about the human body. It will also enable quantum machine learning and neural networks. Like traditional neural networks, quantum neural networks learn from data and make predictions. These are expected to acquire the ability to make decisions with higher precision than current computer and supercomputer-based learning.

Quantum machine learning may be suitable for tasks that traditional machine learning cannot handle, such as complex physics simulations, medical image analysis, and financial risk assessment. Governments and the military could use these capabilities for strategic planning and simulations.

The Quad and quantum internet

To advance the research and development of quantum computing and to promote networking, Quad member countries need to break away from the era of small teams working separately on a country-by-country basis. They should focus on the following challenges:

- Pooling financial and human resources and research capabilities while promoting industrial applications and commercialisation of quantum computing.
- Research and development of QPUs toward FTQC. Rather than focusing only on Quantum Key Distribution (QKD), Quad countries should prioritise the development of the QPUs necessary for developing FTQC and quantum networking.
- Launching a Quad Quantum Network Initiative to promote the unification and harmonisation of international standards for quantum communication technologies, including cryptography and security protocols.
- Building a quantum network that can span the Indo-Pacific, a distance much larger than China's network (which aims to cover a range of the Eurasian continent at least).[1]

Policy recommendations

Cooperation and support in R&D and industrial applications

The governments and enterprises of Quad member countries should cooperate to accelerate the research and development of QPUs towards FTQC and terrestrial and satellite networking. At the same time, research on quantum security should be promoted. Governments should facilitate cooperation by creating frameworks, funding research projects, and establishing bilateral or multilateral agreements.

Quad members should also support measures to promote industrial applications of quantum computing. Governments should work with industry to encourage the use of quantum technology in fields such as finance, medicine, and materials science. Public-private partnerships should allocate funds for R&D, developing quantum computing infrastructure, education and training programs, joint research initiatives, pilot projects, and developing practical solutions for public use. These investments would lead to technological advancements, economic growth, financial gains, and enhanced international influence.

Collaboration for standardisation, security, and regulatory cooperation

The Quad should also serve as a framework for expanding international cooperation on quantum computing. It should work with other international organisations and allied countries to deepen cooperation towards common goals and contribute to establishing international norms and standards. Because quantum computing will significantly impact cryptographic communications, the Quad should also support the development of new security protocols to accompany new cryptographic techniques. International regulations on the military use of quantum technology should be considered.

Support for education and human resource development

Quantum computing and the quantum internet will be fundamental technologies for the next generation, and it is essential to promote human resource development and technology exchange by having security-cleared personnel work together to advance these technologies.[2]

Quad countries should hold joint educational programs and training sessions on quantum computing and the quantum internet to foster the next generation of researchers and engineers and meet the demand in industry and research institutions in each country.

Quad members should also support joint projects on basic research and quantum computing applications and encourage sharing of research results. An environment for sharing the latest knowledge and technologies and learning from each other should be created by establishing joint research facilities and exchanging researchers.

Through the above policy recommendations, Quad countries should work together to promote the development and use of quantum computing and support technological advances for a joint and sustainable future.

Notes

[1] Takahiro, Tsuchiya, "China's Aim for Quantum Hegemony and the Japan-US Alliance", *Issues & Insights Vol. 21, SR 1 – 21st Century Technologies, Geopolitics, and the US-Japan Alliance: Recognizing Game-changing Potential*, HI: Pacific Forum, April 2021, pp.95-106, accessed 22 November 2023, https://pacforum.org/wp-content/uploads/2021/04/issuesinsights_vol-21-SR.1.pdf

[2] Parker, Edward, *Promoting Strong International Collaboration in Quantum Technology Research and Development*, CA: RAND Corporation, 2023, accessed 22 November 2023, https://www.rand.org/pubs/perspectives/PEA1874-1.html

Australian National University | NATIONAL SECURITY COLLEGE

About the author

Takahiro Tsuchiya, Ph.D., is an Associate Professor at the Kyoto University of Advanced Science and a Senior Researcher at the Keio Research Institute at SFC, Keio University.

About this paper

The ANU National Security College (NSC) is a joint initiative of The Australian National University and the Commonwealth Government. NSC is independent in its activities, research and editorial judgment and does not take institutional positions on policy issues. Accordingly, the authors are solely responsible for the views expressed in this publication, which should not be taken as reflecting the views of any government or organisation. NSC's publications comprise peer-reviewed research and analysis concerning national security issues at the forefront of academic and policy inquiry. This paper has been written for the Quad Tech Network Dialogue, held in September 2023 as part of the Quad Tech Network initiative.

About the Quad Tech Network

The Quad Tech Network (QTN) is an initiative of the NSC, delivered with support from the Australian Government. It aims to establish and deepen academic and official networks linking the Quad nations – Australia, India, Japan, and the United States – in relation to the most pressing technology issues affecting the future security and prosperity of the Indo-Pacific.

Contact

national.security.college@anu.edu.au

nsc.anu.edu.au

NSC_ANU

ANU National Security College

CRICOS Provider #00120C

TEQSA Provider ID: PRV12002 (Australian University)