



Cyber resilience for the Quad in a post-quantum world

Jennifer Jackett

Key points

- Advances in quantum computing could jeopardise current encryption methods within the decade, imperilling sensitive data held by individuals, financial institutions and defence and national security agencies in all Quad countries.
- Quad members are well-positioned for collective action to strengthen post-quantum cybersecurity because of their combined quantum talent, research infrastructure, and start-ups.
- Key to this agenda is progressing post-quantum cryptographic standards, strengthening research on the cybersecurity of quantum computing, and bolstering the cyber capacity of regional partners.

Policy recommendations

- The Quad should advance the development of post-quantum cryptographic standards through the Quad International Standards Cooperation Network.
- The Quad should grow the Quad STEM Fellowship program to support scholarship on the cybersecurity of quantum computing.
- The Quad should build awareness of use cases of quantum computing in the region and support quantum-enabled cyber capacity building to help secure critical data and systems.

The coming technological revolution

Advances in quantum computing are expected to transform and disrupt sectors from biomedicine and finance to aerospace and defence. Opportunities and risks abound. Reliable, large-scale quantum computers could address problems like optimisation (for example, finding the best flight path) and enhance machine learning in areas like natural language processing. Quantum computers could answer previously unsolvable math problems that would take a classical computer trillions of years. However, this power could be wielded to undermine factorisation-based encryption, the basis of information security on the internet.





While quantum advances can be subject to hype, experts assess that ‘Q-Day’, or the breaking of current encryption, may arrive within five to 10 years. United States Deputy National Security Adviser for Cyber and Emerging Technology, Anne Nueberger, has described this as a ‘nuclear threat to cybersecurity’.¹ The confidentiality and integrity of sensitive personal, financial, and national security information could be compromised. The operating systems of critical infrastructure may become vulnerable. Spectacular data breaches, like the leaking of almost 10 million Medibank health records in Australia in 2023, would pale in comparison.

This is not a future problem. Hostile state and other nefarious actors have taken the approach of ‘harvest now, decrypt later’. There is an urgent need to secure the data and systems most at risk today among Quad nations and their friends – especially while quantum computing is still nascent. Vital to these efforts is quantum-safe encryption. The US has so far led efforts to

develop post-quantum cryptographic standards.² But many more likeminded countries could play a role, especially in research to test that these standards could withstand hacking attempts.

The superposition of Quad members

Quantum is an opportunity-filled area of cooperation for the Quad, including post-quantum cybersecurity. In the past five years, Australia, the US, Japan and India have all announced ambitious quantum initiatives supported by varying levels of investment (summarised in the table below). Each Quad nation aims to secure its leadership role and harvest the economic and security benefits of quantum technologies. These efforts have hastened in an evolving geopolitical context, where the technological capabilities of competitors such as China in areas like quantum are growing.

			
<p>National Quantum Strategy, including the Australian Quantum Growth Centre and Critical Technologies Challenges Program (2023)</p> <p>Australian Quantum Software Network (2022)</p> <p>Quantum Roadmap (2022)</p> <p>Estimated government expenditure on quantum: US\$100 million (2022)³</p> <p>Global ranking for highly cited quantum computing research: 9th⁴</p> <p>Eight quantum start-ups⁵</p>	<p>National Security Memorandum on Quantum-Resistant Cryptography (2022)</p> <p>The National Quantum Initiative (2018)</p> <p>A National Strategic Overview for Quantum Information Science (2018)</p> <p>Estimated government expenditure on quantum: US\$1.3 billion (2022)</p> <p>Global ranking for highly cited quantum computing research: 1st</p> <p>72 quantum start-ups</p>	<p>Vision of Quantum Future Society (2022)</p> <p>Quantum Technology and Innovation Strategy (2020)</p> <p>Estimated government expenditure on quantum: US\$700 million (2022)</p> <p>Global ranking for highly cited quantum computing research: 7th</p> <p>14 quantum start-ups</p>	<p>National Quantum Mission (2023), including over US\$700 million for research</p> <p>Army Quantum Lab supported by National Security Council Secretariat (2021)</p> <p>Estimated government expenditure on quantum: US\$1.1 billion (2022)</p> <p>Global ranking for highly cited quantum computing research: 13th</p> <p>Six quantum start-ups</p>

Intra-Quad cooperation on quantum technologies has grown both bilaterally and in other groupings. In 2021, Australia and the US signed a Joint Statement of Collaboration on Quantum. In 2022, Australia, the United Kingdom and the US announced the AUKUS Quantum Arrangement. The US-initiated Quantum Economic Development Consortium involves all Quad members.

The interest of individual Quad members in quantum has recently translated through to the shared Quad agenda. In June 2023, the Quad Investors Network launched the Quad Center of

Excellence in Quantum Information Sciences in Melbourne. This is beneficial and long-term work to connect researchers and investors and spur technological collaboration. The Quad could go further by incorporating post-quantum cybersecurity issues into its work program.

A quantum opportunity for the Quad to bolster cyber resilience

The Quad should pursue three complementary initiatives to prepare for a post-quantum world. These build on existing Quad cooperation and have a practical and positive focus drawing on Quad member strengths.

Post-quantum cryptographic standards

Quantum-resistant public key cryptographic algorithms are essential to secure data and systems in a post-quantum world. The US, through the National Institute of Standards and Technology, is leading global efforts to solicit, evaluate and standardise one or more quantum-resistant algorithms. The Quad should use its International Standards Cooperation Network to engage academia and the private sector in the development of these standards. Quad nations should convene a roundtable in 2024 on post-quantum cryptography standards and agree a roadmap to accelerate their development and implementation.

Quantum STEM fellowships

The impact of large-scale quantum computers on cybersecurity is an under-researched area. It is important that, as efforts to develop quantum computers advance, security considerations are incorporated into the design process. Drawing on the collective quantum research talent of Quad members, the Quad should develop a second phase of the STEM Fellowship program. This should support scholarship on the cybersecurity of quantum computing. Research should cover both how to secure cyber systems against quantum computers and how to use the power of quantum computing to detect and deflect cyberattacks.

Regional cyber resilience

Quantum computing-related research, infrastructure and investment is concentrated in the most advanced economies. Less developed partners in the Indo-Pacific do not necessarily have the resources or expertise to secure their data and systems to mitigate the cyber risks of quantum computing. The Quad should have a two-pronged quantum capacity-building plan for the region, led by the Quad Senior Cyber Group. The first track should focus on awareness raising about quantum computing use cases and the implications for cybersecurity. The second track should provide on-the-ground support to partner governments and businesses to strengthen their cyber defences.

Notes

¹ Swayne, M. 'Nuclear Threat to Cybersecurity' – Post-Quantum Cybersecurity Rapidly Gains Attention of U.S. Congress, Administration (2022), *The Quantum Insider*, accessed 21 November 2023, <https://thequantuminsider.com/2022/07/25/nuclear-threat-to-cybersecurity-post-quantum-cybersecurity-rapidly-gains-attention-of-u-s-congress-administration/>

² National Institute of Standards and Technology, 'Post-Quantum Cryptography' (2023), accessed 21 November 2023, <https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization>

³ All estimates of government expenditure on quantum information sciences sourced from Washington Technology Industry Association, *Quantum Information Sciences in Washington State: A Technology Landscape Report* (2023).

⁴ All rankings for highly cited research in quantum computing sourced from the Australian Strategic Policy Institute, Critical Technology Tracker (2023) , accessed 21 November 2023, <https://techtracker.aspi.org.au/tech/quantum-computing/?c1=us>

⁵ All figures on number of quantum start-ups sourced from McKinsey & Company, *Quantum Technology Monitor* (2023)



Australian
National
University

NATIONAL
SECURITY
COLLEGE

About the author

Jennifer Jackett is a Sir Roland Wilson Scholar at the National Security College, Australian National University. The views expressed are solely those of the author.

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)