POLICY BRIEF

Security in a Post-Quantum World: *Australia's Strategy for the Future*

August 2017

Nathan Arnold, Sabina Baunin, Niamh Cunningham, Daniel Tasso and Alex Vipond

YOUNG AUSTRALIANS in INTERNATIONAL AFFAIRS

Security in a Post-Quantum World: *Australia's Strategy for the Future*

By Nathan Arnold, Sabina Baunin, Niamh Cunningham, Daniel Tasso & Alex Vipond

Image credit: US Department of Defense (Flickr: Creative Commons)

Executive Summary

Ensuring Australia is well-positioned to take advantage of developments in quantum computing requires development of a coherent strategy, and cross-departmental policy coordination. However, Australia must first overcome the challenges of having no clear, existing strategy, and the need to temper a focus on technological gains with the need to protect Australia's interests online. In order to seize opportunities and overcome the aforementioned challenges, three key recommendations are emphasised to policymakers. First, policymakers should embed quantum security into the Australian Cyber Security Strategy moving forward. Second, building upon this foundation, this brief recommends that the Australian government establish a National Quantum Security Centre to drive this strategic policy direction, coordinate resources and support research. Third, the development of a strategic framework for public and private sector cooperation will enable the Government to harness the strengths of both sectors, and cultivate a skilled workforce to help Australia establish itself as a security leader in a post-quantum world. These steps will ensure the country is prepared for the coming evolution in computing, and can defend against the security threats it may bring.

Background

There is a technological evolution under way in computing. Across the world, countries including the United States, China and Russia and companies such as Alibaba, Google and IBM are investing millions of dollars in quantum computing. With traditional computer chip processing-power reaching its limits, quantum computers represent the next phase in computing power. While a traditional computer allows information to exist in the binary state of 1 or 0, quantum computers allow information to exist in multiple states (both 1 *and* 0).

It is this power that enables a quantum computer to search extraordinarily large quantities of information and factor enormous mathematical problems at speeds much faster than any traditional computer. In countless fields of research and exploration—artificial intelligence and medicine for example—these computers offer solutions to complex problems that were previously constrained by time. Recognising this potential, several concept machines are already in use in universities and tech companies.

Quantum computing offers potentially-unlimited avenues for global advancement. But it is this strength, particularly at factoring, that has the capacity to break the algorithmic standards which form public key cryptography. This means that some computer systems could be vulnerable to exploitation by criminals, hackers or even terrorist groups.

Why is this important?

Public key cryptosystems underpin the internet's security. These cryptosystems authenticate and secure communications between a computer and the internet over networks (e.g. email) and software downloads. Cryptosystems are responsible for securing billions of connections every day and as internet penetration rates and the volume of internet-capable devices continue to grow, this responsibility will only multiply.

An internet that is not secure exposes data and systems to exploitation, theft or destruction. Experts predict it will take 15 years to build to a quantum computer with enough processing power to break the world's most potent algorithms that make up these cryptosystems. To counter these risks, a new industry of quantum-resistant or post-quantum cryptography is emerging.

The Australian government has recognised the importance of this field. It has invested in quantum research through the Australian Research Council's Centre for Engineered Quantum Systems (EQUS) and Centre for Quantum Computation and Communication Technology.

The Challenge

The challenge for Australia now is to position itself to take full advantage of this quantum revolution rather than be exposed to its risks.

The government has invested some resources into the field of quantum computing and advancing a national call for 'better focused cyber research and development'. But Australia does not currently have a quantum security strategy in place.

If Australia's cryptosystems were to be broken, it would compromise the nation's cyber security on an unprecedented scale. It could potentially expose government, business and citizens to serious risks. Without a formal and proactive strategy on quantum security, Australia is vulnerable and may have to deal with new and advanced cyber threats with limited resources and capabilities.

The power of quantum computing and its potential impacts on cyber security mean that it is imperative that the Australian government develops a multi-faceted strategy that secures the nation's future.

Recommendations

For the Australian government to adequately respond to the financial, informational and national security threats posed by the post-quantum world, this brief recommends the following be adopted by the Federal Government as part of its wider cyber security strategy:

1. Embed quantum security as a key objective of Australia's Cyber Security Strategy

In April 2016, Prime Minister Malcolm Turnbull officially launched the Federal Government's 'National Cyber Security Strategy'. Detailing over 30 new initiatives worth $231 million, the cyber strategy sets out the government's 'philosophy and program for meeting the dual challenges of the digital age', namely, advancing and protecting Australia's interests online. To achieve this, the cyber strategy establishes five key 'themes of action', including a national security partnership, strong cyber defences, global influence, growth and innovation, and a cyber smart nation.

It is recommended that the Federal Government integrate quantum security—and quantum cryptography in particular—as a core objective of this cyber security strategy. Inclusion of quantum security would enhance national security, send a signal of support to Australian businesses in this sector and give Australia the opportunity to carve a foothold in a potentially revolutionary industry.

2. Establish a National Quantum Security Centre

It is recommended the Federal Government establish a National Quantum Security Centre. This would be responsible for the coordination and policy direction of Australia's quantum research and development as it relates to security. A national centre would greatly enhance the government's ability to develop Australia's knowledge base and human capital in the industry, as well as allocate resources across the sector efficiently. In accordance with Australia's 2016 *Cyber Security Strategy*, the quantum research centre should form under the guidance of Data61—a digital research unit at CSIRO. Data61 is tasked with 'growing [Australia's] cyber security innovation, with particular focus on technical capabilities', so it could oversee the establishment of such a centre.

Over the past decade, Australia has played a critical role in the development of quantum research and technology. In some areas of research, including quantum processor manufacturing, it has emerged as a global leader. Since its inception, Australia's 'quantum industry' has been largely concentrated around a handful of university-based, national research centres that are co-funded by the Federal Government, private sector entities and international donors (including the United States). Two of the most prominent

centres are the Centre of Excellence for Engineered Quantum Systems (EQuS), which was established in 2010, and the Centre of Excellence for Quantum Computation and Communication Technology (CQC2T), based at the University of New South Wales. In 2016, through the National Innovation and Science Agenda, the Turnbull Government committed to contributing $25 million over five years to the development of these two centres alone. The government's investment was also complemented by $25 million from various partnering Australian universities, and $10 million from the private sector in a $70 million agreement between the research community, business and the Federal Government.

While Australia's research facilities have been responsible for critical breakthroughs in advanced quantum computing, it is imperative to note that EQuS and CQC2T also operate as independent organisations. As a result, despite technically falling under a single Commonwealth entity, Australia's 'quantum industry' suffers from a general lack of common research objectives and shared strategic direction. This absence of any centralised leadership undoubtedly represents an important obstacle in the development of a comprehensive quantum security strategy. The establishment of the National Quantum Security Centre as a centralised body therefore represents a necessary response to this challenge.

3. Develop a strategic framework for public and private sector cooperation

This brief's third recommendation identifies key areas to enable the development of a strategic framework between the public and private sectors as a strong foundation for Australia's post-quantum security sector.

Developing the National Quantum Security Centre (NQSC) as a networking hub:

The banking and audit sectors in addition to cyber-security and software companies should be encouraged to form collective partnerships with government entities such as the Australian Signals Directorate under the umbrella of the NQSC. Together, these industries can benefit from regular contact with one another, and collectively access the resources of the NQSC as a hub for collaboration. The focus of this collaboration will be the new and emerging issues that arise as quantum computing evolves; a space where leaders across multiple sectors can communicate openly and assess their needs.

Through this hub, businesses will be encouraged to develop partnerships with industry leaders, such as Quintessence Labs, to continue research into cryptographic products, and with EQUS, the cybersecurity arm of Data61 and SINET, to develop human capital.

This would enable industries to share developments and help frame the strategic direction of future research, investment and outsourcing opportunities. Public and private

representatives would be encouraged to collaborate regularly and set objectives for each meeting.

Seek talent through universities and existing sectors:

Both the public and private sector have an incentive to invest in the human capital required to meet their needs in the next decade. Public and private collaboration with the education sector should offer professional and technical development opportunities, incentivising young Australians to seek employment in quantum security. This can be achieved through these industries reaching out to students in universities, and by holding competitions such as 'hack-a-thons' to attract talented and motivated individuals with industry potential. This approach would see additional funding, partnerships and the development of human capital required to create a sustainable quantum security sector.

Both the public and private sectors will see advantages by collaborating on talent seeking initiatives within universities and across other sectors. By encouraging those with the highest potential to pursue careers in quantum computing, government and business alike will proactively address proactively address potential skills shortages in their sectors.

The National Quantum Security Centre to expand to multiple locations:

Over the next decade, as advancements in the field of quantum computing are made (justifying increased resourcing by the government), it is recommended that that NQSC be expanded to multiple locations across the country. This will enable closer partnership with businesses, as locations can capitalise on CBD locations (and their talent pools) nationwide.

This long term objective would underscore Australia's ongoing commitment to being a world leader in the field of quantum computing.

Develop Sustainable Recovery Plans:

As part of enhancing public-private partnerships in this space, government and businesses are encouraged to develop comprehensive and flexible disaster recovery plans to address any emerging vulnerabilities of new encryption methods.

Organisations can benefit from developing comprehensive digital forensic methods, which will aid in building an adaptable response to the evolving post-quantum frontier. This recovery and continuity planning will help prioritise spending in both the public and private sector. For example, an investment in software such as True Random Number Generator—which creates highly complex cryptographic keys and has no back doors

vulnerable to cyber-criminal access—may be justified as helpful in adapting successfully in a post-quantum security framework.

Conclusion

The significance of quantum computing and its potential to impact the cyber security of all Australians cannot be understated. In developing a coherent quantum computing strategy, the Australian Government will position the country to take full advantage of this evolution, rather than be left vulnerable to it. This brief proposes that the Federal Government embed quantum security as a key objective of Australia's long-term cyber security strategy. Central to this objective, it is recommended that the Federal Government establish a National Quantum Security Centre to coordinate and drive the policy direction of Australia's quantum research and development as it relates to security. Further, it is recommended the government develop a strategic framework for public and private sector cooperation to enable policymakers and businesses alike to maintain pace with the developments in this field and the security ramifications. These recommendations, if undertaken, will empower the policy direction and coordination needed to prepare Australia for the future of cyberspace.