The Quantum Threat to Cyber Security: Danger and Opportunity

Submitted in support of a presentation to the Standing Committee on Public Safety and National Security regarding Cybersecurity in the Financial Sector as a National Economic Security Issue

Dr Michele Mosca, Brian O'Higgins, and Bill Munson, Quantum-Safe Canada

February 22, 2019

1. Canada's *National Cyber Security Strategy and the Quantum Threat*

Canada's cybersecurity strategy, *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age* (June 2018) stresses the need to prepare for increasingly sophisticated threats to the cyber systems relied on by our critical infrastructure and democratic institutions. The Strategy commits the government – in this context its cybersecurity efforts – to "focus on emerging areas of Canadian excellence, such as quantum computing".

Most of us have heard of quantum computing, know that it's coming, and are aware that it will bring an almost unimaginable speed-up in the ability of computers to perform calculations. This will enable wonderful advances in, for example, our ability to discover new materials and design new life-saving drugs. Unfortunately, powerful quantum computers will also enable the hacking of today's 'unbreakable' encryption in minutes.

As things stand, the encryption that underpins the security of society's critical infrastructure is at serious risk of being undermined by quantum computers within the next 8-15 years. This is the quantum threat – that Canada's national security and economic prosperity will be jeopardised as government, communication, transportation, banking, energy and other critical systems become vulnerable to hostile actions because our cryptography is no longer strong enough to protect us. Even now, bad actors are able to copy and store encrypted data until a quantum computer is available to decrypt it.

We outline here how achieving a quantum-safe Canada is a natural cornerstone of a Canadian strategy to protect Canadians and our economy from cyber attacks, while reaping economic benefits from those efforts.

1. The Quantum Threat to Cybersecurity

There is increasing recognition of the need for society to prepare for increasingly sophisticated threats to the cyber systems that are relied on by our critical infrastructure and democratic institutions. This will require substantial investments in cybersecurity tools, services and skills, including those necessary to address the quantum threat.

At the same time, cybersecurity is not only a means of protection, but also an important source of innovation that will help ensure competitiveness. There are calls for governments to focus efforts on supporting emerging areas of local, regional or provincial excellence – and in Canada this clearly includes quantum computing.

2. Addressing the Quantum Threat

Canada must respond proactively to the quantum threat, implementing the elements that will enable an orderly and timely transition to quantum-resistant cryptography. If we don't, our security and economic prosperity will be jeopardised as government, banking, energy, artificial intelligence and other critical infrastructure systems become vulnerable to hostile actions because of weak cryptography.

The most common form of cryptography – that used in public-key infrastructure – is also the most vulnerable. This is a source of great concern, as its uses have universal importance – key agreement (so that only the intended parties have access to a specific communication or transaction) and authentication (so that each party to a transaction knows that the other parties are who they say they are, and that messages are legitimate). Without such assurances, there will be no trust online and few transactions, whether they involve humans or the devices that make up the internet of things.

The challenge is that a replacement suite of mature, tested quantum-resistant cryptographic algorithms is not yet available. Nor are the tools based on them. Nor are the cybersecurity experts with quantum-safe skills who will use the tools to diagnose and fix each system separately. Without a strong impetus to focus efforts on a long-term campaign to meet the quantum threat, Canada will lose ground as vulnerabilities are exploited and the potential for global leadership is undermined.

3. Quantum-Safe Solutions

An effective response to the quantum threat will necessarily involve a range of stakeholders working together to identify opportunities to translate their research into innovative quantum-safe products. An infusion of targeted financial support for infrastructure and personnel is needed to accelerate work on the discovery, testing and deployment of quantum-safe solutions in two areas – post-quantum cryptography and quantum key distribution.

3.1 Post-Quantum Cryptography

Quantum readiness demands that new quantum-safe algorithms and cryptographic tools be discovered and developed to replace those now in place. In 2016, the US National Institute for Standards and Technology (NIST) began a multi-year project to identify a standardised suite of viable quantum-resistant cryptographic systems by 2024. The announcement of NIST standards for post-quantum cryptography is expected to result in a retooling of the ICT infrastructure worldwide.

Canadian researchers are active in the NIST effort, and have contributed a number of the candidates now under consideration. It will be to Canada's long-term economic advantage if our researchers participate centrally at every stage of the NIST process and beyond, and their efforts should be encourage and supported.

Canada's researchers and technologists are also at the forefront in developing software and services for post-quantum cryptography, including open-source software, commercial software and consulting services. In response to advances in quantum computing, researchers will need to continue their work as successive generations of increasingly efficient and effective quantum-safe cryptography are deployed.

3.2 Quantum Key Distribution

Research and development of practical quantum key distribution (QKD) requires substantial investment in essential physical components – such as satellites and ground stations – as well as skilled personnel. The goal is a scalable, tamper-proof QKD tool that uses properties of quantum science to protect the all-important key agreement that commences digital transactions.

There is a clear need for QKD to be integrated into a real-world network in 3-5 years. This would enable the testing of QKD with a national satellite-based network linking individual collaboration centres. Preliminary work is already underway at universities across Canada. Not only are some of the key physical elements in place, but key researchers have already coalesced and can mobilise quickly.

These researchers will continue innovating to make QKD more effective and less expensive. What they need is additional financial support so they can accelerate this work to address the impending threat. This would likely first entail the completion of several collaboration centres on separate networks, the most likely centres being:

- Calgary (near energy sector; to be enhanced)
- Waterloo / Toronto (near financial sector and government; to be developed)
- Ottawa (near government; to be completed)
- Quebec (tied, for example, to aerospace or the AI sector; to be developed).

The separate networks would subsequently be integrated into a single functioning Canadian QKD network, which may eventually be linked into a global QKD network.

4. <u>Expanding the Quantum-Safe Skills Base</u>

The National Cyber Security Strategy recognises the need to expand Canada's capacity to undertake the requisite research and commercialisation activities. Serious steps must be taken to strengthen and expand Canada's skills base, without which the desired facets of cybersecurity – protection and economic development – cannot be achieved.

Programs and courses offering professional training will need to be established if Canada is to have the necessary cadre of cybersecurity experts with superior quantum-safe skills. These experts would perform tasks such as cyber risk assessment and systems integration to ensure that the appropriate quantum-safe solutions have been properly installed and integrated into complex legacy systems.

Development of the necessary large pool of systems integrators and cybersecurity consultants with strong quantum-safe skills will take several years. A number of Canadian colleges have indicated interest in augmenting their cyber-security programs with courses focusing on the migration to post-quantum cryptography. Ideally they will collaborate on a standard quantum-safe module for incorporation into existing cybersecurity programs.

In addition, possibilities around outreach to industry should be explored. There is likely to be an appetite for training courses to familiarise technical staff with quantum-safe technologies and how best to work with external quantum-safe experts. There will also be a need for certification schemes by which the quality of the training and the expertise of the trainee may be evaluated.

While education is a provincial responsibility, there is a need for the federal government to play strategic and funding roles to ensure that the provinces and territories (and the agencies and regulatory bodies they control) move with a sense of urgency.

5. Using Government Policy Levers

Governments have access to numerous policy powers that may be useful in encouraging and even ensuring that digitally enabled infrastructure – such as smart roads, smart bridges and smart cities – is designed, built and installed to be quantum-safe. These levers include approval, planning, procurement and funding powers, none of which needs to be costly.

A simple example would be a federal policy that any proposal for federal support for an infrastructure project must be accompanied by a cybersecurity strategy. This would necessarily include a quantum-safe strategy for infrastructure expected to be in service for decades.

6. Taking Advantage of Opportunities for Canadian Leadership

As noted above, the National Cyber Security Strategy stresses the need to prepare for increasingly sophisticated threats to the cyber systems. At the same time, it points out that cybersecurity is not just a means of protection, but also an important source of innovation that will help ensure Canada’s competitiveness. Both sides of the coin are in play when it comes to the quantum threat.

Working in our favour is the fact that Canada is in the vanguard globally in both cryptography and quantum-information science, and strong in cyber security. There is a significant history of collaboration among these realms, so we should be able to get our house in order ahead of other countries and then export our quantum-safe products and expertise abroad. Canada's national security and economic prospects will both be enhanced if we take advantage of this opportunity.

Implementation of the key elements discussed above will enable Canada to take advantage of the opportunities for innovation, prosperity and competitiveness that are inherent in moving quickly to address the quantum threat. A number of complementary actions should also be taken in support of the core elements:

- Naming an advisory committee of top scientists in cryptography and cybersecurity to provide expert advice on research priorities and parameters for projects and proposals.
- Identifying the technical expertise needed to monitor relevant international standards-development work, participating as necessary.
- Identifying the program-management expertise to advance innovation and commercialisation activities, market-research exercises to quantify the national and global requirements for quantum-safe expertise, and export-development initiatives related to quantum-safe technology, expertise and training.

Without a strong push to focus efforts on a long-term campaign to meet the quantum global leadership is undermined. We cannot afford to be a follower, facing massive security vulnerabilities and prohibitive upgrading costs simply because we delayed taking action. At the same time, we should not be blind to the economic benefits of vibrant cybersecurity and quantum-safe industries, or to the danger that we will lose our current edge if we delay action.

7. List of Recommendations

- That the Committee urge the Government to emphasise the need to respond vigorously to the quantum threat. Otherwise, our security, competitiveness and economic prosperity will be jeopardised as government, banking, energy, artificial intelligence and other critical infrastructure systems, including those that support our democratic institutions, become vulnerable to hostile actions because of weak cryptography.
- That the Committee urge the Government to respond proactively to the quantum threat, putting in place the elements needed for Canada to become quantum-safe in an orderly and timely manner. The key elements calling for government funding support are targeted research into quantum-safe cryptography, ongoing development of quantum key distribution via satellite, and the creation of a robust talent pipeline to generate the necessary cadre of cybersecurity experts with superior quantum-safe skills.

- That the Committee urge the Government to use policy levers at its disposal – including approval, planning, procurement and funding powers – to ensure that digitally enabled infrastructures such as smart roads, bridges and cities are designed and built to be quantum-safe.

- That the Committee urge the Government to provide suitable funding to a not-for-profit entity that is able to initiate and oversee the multi-faceted work needed for Canada to implement a robust quantum-safe strategy. Such a strategy must both secure our critical infrastructure and take advantage of the opportunities for innovation, competitiveness and prosperity that are inherent in moving quickly to address the quantum threat. Quantum-Safe Canada is willing and able to serve in such a capacity.

Dr Michele Mosca is an award-winning researcher in cryptography and quantum computing, and has initiated numerous multi-disciplinary collaborations that helped create the quantum-safe opportunity for Canada. He started and grew the quantum computing effort at Waterloo, eventually co-founding the Institute for Quantum Computing. He led the first Canadian research network in quantum computing, he drove the establishment of the quantum computing graduate program at Waterloo and the Quantum Cryptography Summer School for Young Students for high school students, was a founding member of Perimeter Institute, co-founded two start-ups, and co-founded the ETSI-IQC Quantum-Safe Cryptography Workshop series. Most recently he co-founded and is the Director of Quantum-Safe Canada.

Brian O'Higgins is an angel investor and board member with over 30 years of experience as a leader in security technology development. He is perhaps best known for his pioneering role in public key infrastructure and as the co-founder and Chief Technology Officer of Entrust, a leading internet security company. He was also a co-founder and Chief Technology Officer of Third Brigade, an enterprise security company that was acquired by Trend Micro in 2009. His current list of affiliations includes advisory board positions with Defence R&D Canada, the Ontario Centres of Excellence, and as an Executive Fellow with the Mistral Venture Partners fund. He also serves as Chair of the Board of Directors of Quantum-Safe Canada.

Bill Munson is Director, Research and Policy Analysis at Quantum-Safe Canada. He is a policy analyst who, prior to joining Quantum-Safe Canada, spent more than 20 years with the Information Technology Association of Canada, where he established and ran the highly regarded ITAC Cyber Security Forum from 2000 to 2015.

Quantum-Safe Canada was established in 2017 to raise awareness of the quantum threat and to help coordinate the development of the research, technology, tools and training needed to transition successfully to quantum-resistant cryptography. Our vision is based on a twin focus – security and prosperity.

Quantum-Safe Canada possesses an impressive foundation of knowledge and ability, and is committed to collaborating with government and others to respond effectively to the impending quantum threat. Registered as a not-for-profit and with an impressive Governing Board, Academic Steering Committee and Industry-Government Advisory Council already in place, Quantum-Safe Canada is uniquely positioned to contribute meaningfully to efforts ensuring that domestic critical infrastructure systems are protected and that Canada's capabilities are marshalled into global leadership and economic advantage.