The Quantum Threat and Curriculum Development in Canada

2022 07 11

The Quantum Threat to Cybersecurity

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.

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). This extends the quantum threat into every digitally connected business and household in Canada.

Addressing the Quantum Threat

Canada must respond proactively to the quantum threat, implementing an orderly and timely transition of our digital infrastructure to quantum-safe cryptography. If we don't, our security and economic prosperity will be jeopardised as our critical infrastructure systems become vulnerable to hostile actions because of weak cryptography. This transition requires not only technological solutions but also reliable processes and skilled personnel to design, implement and manage them.

Expanding the Quantum-Safe Skills Base

Unfortunately, we lack a workforce with the quantum-safe skills needed to diagnose and fix the breadth of vulnerabilities. Without a determined campaign to strengthen and expand our quantum-safe skills base, Canada will lose ground as vulnerabilities are exploited, systems and information are compromised.

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. While the existing workforce will in most cases understand their organizational challenges and requirements, outside experts will be relied on to perform tasks such as cyber-risk assessment and systems integration to ensure that appropriate quantum-safe solutions have been properly integrated into complex legacy systems.

A number of Canadian colleges have shown interest in augmenting their 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. There is also likely to be an appetite for training courses and other learning activities to familiarise technical staff with quantum-safe technologies and how best to work with external quantum-safe experts. In addition, business leaders will need to understand the risks to their organizational security so that they can direct appropriate investment and action.

Efforts taken by Quantum-Safe Canada

Quantum-Safe Canada is a not-for-profit established in 2017 to raise awareness of the quantum threat and lead efforts to strengthen Canada's research, innovation, commercialisation and talent pipelines. With respect to the latter, Quantum-Safe Canada is already laying a solid foundation for the development and introduction quantum-safe courses and programs.

First, a project was launched to identify and describe relevant work roles and general curricular requirements supporting the integration of quantum-safe technologies within Canadian enterprises. This resulted in a 65-page report titled *Organizational Migration to Quantum-Safe Cryptography: A Role-Based Framework, Learning Outcomes and Curriculum Model*, published in March 2022.

A second project is now underway to develop a curriculum guide that will include a project-based curriculum design for each major role (senior leader, tech advisor, business advisor, tech expert), and sequencing of learning activities that support the functional requirements (planning, integrating, implementing, managing). The guide is expected to facilitate adoption of quantum-safe content into a wide range of types of programs, including the following: short-cycle courses, continuing education programs; college / university certificate programs; longer degree and diploma programs; and stand-alone quantum-safe certificate or micro-credential programs. This work will be wrapped-up later this calendar year.

In both projects, impressive groups of experts from industry, government and academia – including curriculum-development experts – have provided valuable guidance.

Next Steps

It is clear that the missing piece is actual curriculum(s). Our track record shows that Quantum-Safe Canada is well placed and more than capable of leading and administering an effort to develop quantum-safe curriculum for any or all of the types of quantum-safe programs listed above. However, Quantum-Safe Canada will need a serious funding partner given the costs involved in working with a representative group of curriculum experts across the country. Expressions of interest in the work will be gratefully accepted.