

Thoughts on *Developing a National Quantum Strategy*: Focusing on the Quantum Threat to Cybersecurity

Quantum-Safe Canada is pleased to respond to the questions posed in *Developing a National Quantum Strategy: Engagement Paper* and at a subsequent security roundtable hosted by the National Quantum Strategy secretariat.

Although Quantum-Safe Canada (QSC) is deeply interested in quantum technologies and the quantum industry in general, we have chosen to discuss and respond to the questions with a narrower focus – what Canada needs to do to prepare to respond effectively to the quantum threat to cryptography. A quantum strategy that does not ensure that digital systems will be quantum-safe in time will undermine the quantum-computing sector and the value it can bring to its customers.

There is broad awareness that quantum computing 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, full quantum computers will also enable the hacking of today's 'unbreakable' encryption in hours and minutes – instead of thousands of years, as is currently the case.

As things stand, the encryption that underpins the security of society's critical infrastructure is at serious risk of being undermined by quantum computers, perhaps even 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.

The most common form of cryptography – that used in public-key infrastructure – is also the most vulnerable to the quantum threat. 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.

Canada must respond proactively to the quantum threat, implementing the elements that will enable an orderly and timely transition to quantum-resistant cryptography. 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 assess risk and 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.

The quantum threat will be the focus of our remarks in the following pages. The text in italics is from the government documents – principally the questions, but occasionally the preamble to a question. QSC's responses are in regular font, with recommendations in bold.

Thoughts on *Developing a National Quantum Strategy:* Focusing on the Quantum Threat to Cybersecurity

Questions from the *Engagement Paper – July 15, 2021*

Question 1. Which applications and research areas offer the greatest potential for Canadian researchers and firms to strengthen their leadership to succeed globally? What stretch goals and priorities can be set for these applications in the next three years and beyond to make a roadmap for a leap forward?

- The downside of quantum computing is the threat it poses to the current cryptographic base; if the threat has not been addressed first, there is a very high probability of not realizing the upside.
- This is a critical matter both for national security perspective and for a broad quantum industry that is looking for support, funding and adoption.

QSC Recommendations

- 1. The three-year goal for the Government of Canada should be serious movement towards a quantum-safe Canada, including aggressive programs to raise threat awareness and encourage investments in standards development and cryptographic agility, and an approach to the development of the implementation skills base needed to achieve quantum readiness.**
- 2. The longer-term goal should be the broad achievement of cross-Canada quantum readiness, incorporating migration from traditional to post-quantum cryptography and perhaps quantum key distribution.**

Thoughts on *Developing a National Quantum Strategy*: Focusing on the Quantum Threat to Cybersecurity

Question 2. How can academia, industry and government work better individually and collectively to accomplish national objectives in quantum technologies?

QSC Recommendations

- 3. Efforts should focus on security from quantum computing, and not just security of quantum computing.**
- 4. Government should work from a short set of national objectives rather than a funding wish list, and should have a clear roadmap to achieve those objectives.**
- 5. The first objective should be to bring Canadian critical infrastructure to a position of resilience against quantum-enabled attacks through technology-lifecycle management.**
- 6. A key point here is that the Government should be much more vigorous in using its procurement, approval and funding powers to encourage, and eventually compel, the adoption or inclusion of quantum-safe technologies, products and practices that government purchases, approves or funds.**
- 7. The second objective should be to save and create jobs and bring economic growth through a strong Canadian quantum-safe industry sector; to this end, the Government should consider targeted initiatives related to funding quantum-safe R&D and commercialization initiatives, skills development and export promotion (as discussed and recommended elsewhere in this document)**
- 8. Implementation should be funded through flexible vehicles that allow different elements to be funded differently.**

Thoughts on *Developing a National Quantum Strategy:* Focusing on the Quantum Threat to Cybersecurity

Question 3. What are the key challenges and opportunities for academia and industry in the development, attraction and retention of talent?

- Canada needs to produce more talent through education and training; currently, quantum-safe concepts are only touched on in a few specialized departments in academia.
- Curriculum for a broader cross-section of academic and technical programs should include understanding cryptography and risk, and provide tangible advice on, for example, using lifecycle management to smooth the costs of upgrading.
- The talent required for quantum readiness is not just scientific researchers in academia, industry and government, but also significant numbers of risk-assessment, systems-integration and cybersecurity professionals with quantum-safe skills.
- The completion of cryptographic migration across all sectors of the Canadian economy will take more talent than currently exists; while some organizations are looking for serious conversations on how to address this gap, much more discussion is required – and should be fostered.
- Canada also needs to do more to retain the talent we have; we appear to be losing quantum-related talent to more competitive countries – and therefore opportunities to grow Canada's quantum sector.

QSC Recommendations

- 9. The Government should encourage provinces and territories to integrate material regarding cybersecurity, cryptography and the quantum threat into the curriculum of a wider cross-section of educational institutions, including universities, technical colleges and CEGEPs.**
- 10. This should be done on an accelerated basis to ensure that the necessary quantum-safe cybersecurity skills are available when they are required to combat the quantum threat.**
- 11. Industry should be encouraged, perhaps through matching or other funding programs, to collaborate to establish and support training programs targeted at cybersecurity and risk-management students and professionals with an interest in upgrading their skills to include quantum-safe concepts.**
- 12. The Government should introduce targeted incentives to encourage industry to get involved in education and training through offering internships to academic trainees in cybersecurity, cryptography and quantum cryptography.**

Thoughts on *Developing a National Quantum Strategy:* Focusing on the Quantum Threat to Cybersecurity

Question 4. What can be done to ensure that, as Canada's quantum sector grows, it is increasingly representative of our diversity?

- As a relatively new field of both academic and entrepreneurial endeavour, quantum readiness seems less burdened by unfair and unproductive legacy hierarchies and practices than many other fields are, and consequently more open to contributions from a diversity of sources.
- For example, the Quantum Cryptography School for Young Scientists at the University of Waterloo's Institute for Quantum Computing welcomes a gender-balanced cohort of high-school students from diverse backgrounds.

QSC Recommendation

- 13. Institutions should be encouraged to focus on maintaining this openness and weaving it throughout the education and training framework in their efforts to develop and retain talent (as discussed above under question 3), and to develop quantum-safe course materials and 'train the trainers' (as discussed below under questions 15 and 16).**

Thoughts on *Developing a National Quantum Strategy: Focusing on the Quantum Threat to Cybersecurity*

Question 5. What are the greatest opportunities and challenges in commercializing quantum innovations in the Canadian context? Do different quantum technologies (e.g., sensing and imaging, computing hardware, algorithms, communications, and materials) require specific approaches?

- A challenge for commercialisation across the quantum industry (including the quantum-safe sector) is that Canada's government-procurement practices have often been a barrier to uptake by the country's largest domestic market, the public sector. Turning this situation around would create a major opportunity.
- There also appears to be a trend for some successful Canadian start-up companies to sprout here and then move to the United States, Israel or the European Union for a variety of reasons, including tax calculations and other benefits.
- These are Canadian ideas and Canadian talent that are lost to other jurisdictions, and there is no reason to think that the quantum-safe sector will be an exception.
- There is no doubt that some, if not all, of those departing start-ups would have chosen to stay in Canada if changes had been made to existing Canadian policies.
- We commend the Business Development Bank of Canada for introducing its Deep Tech Venture Fund, which includes quantum technologies.

QSC Recommendations

- 14. The Government should leverage its role as a significant commercial customer by encouraging early testing, purchase and deployment of the products and services of Canada's quantum-safe start-ups – in its own operations and across the economy; this might include subsidies for companies purchasing such products and services.**
- 15. Government agencies and programs should dedicate additional funding to programs like Innovative Solutions Canada, which encourage quantum-safe start-ups to run proof-of-concept and pilot projects.**
- 16. These programs should also provide funding to support and encourage private companies to run such projects; results could be publicized, with participating companies receiving support to grow into larger projects and commercial deployment.**
- 17. The Government should also introduce targeted incentives for quantum-safe research, R&D and commercialization in the interests of both national security and economic development, the two thrusts of Canada's *National Cyber Security Strategy*.**

Thoughts on *Developing a National Quantum Strategy*: Focusing on the Quantum Threat to Cybersecurity

Question 6. How can the National Quantum Strategy help to ensure that, as quantum technologies and solutions come to fruition, they are adopted by Canadian businesses, academia, government and the public?

- Broad adoption of quantum-safe measures is very much in the interests of both national security and industrial development and economic prosperity.

QSC Recommendations

- 18. The National Quantum Strategy should encourage government departments to use their procurement, approval and funding powers to ensure that their systems and those of other critical infrastructure sectors – especially regulated sectors – are designed, built and implemented to be quantum-safe (see Recommendation 6 above).**
- 19. Government-procurement practices should be amended to favour Canadian quantum-safe products and services, incentivizing companies to stay and grow in Canada.**

Thoughts on *Developing a National Quantum Strategy: Focusing on the Quantum Threat to Cybersecurity*

Question 7. How can the National Quantum Strategy best address the societal, ethical, legal and policy considerations that may arise given quantum technologies' disruptive capability?

- In some ways, the quantum threat appears to be the ‘killer app’ of quantum computing – literally as well as figuratively; to unleash quantum computing without having first ensured widespread preparedness for the concomitant quantum threat seems irresponsible.
- Some government departments have made strides in the quantum-safe arena – most notably the Canadian Centre for Cyber Security, which has been doing valuable work for some time, and Public Safety Canada, which flagged the quantum threat in the National Cyber Security Strategy and has provided project-specific funding to QSC.
- QSC is also happy to acknowledge the following: the Office of the Superintendent for Financial Institutions’ inclusion of the quantum threat in a recent discussion paper; the strong support of Innovation, Science and Economic Development staff in the development of best practices for the finance sector under the Canadian Forum for Digital Infrastructure Resilience (CFDIR); the Bank of Canada’s active participation in the CFDIR work; the Treasury Board Secretariat’s willingness to consider working quantum-safe requirements into its procurement framework; Infrastructure Canada’s apparent openness to take cybersecurity and quantum readiness into account in undertaking the recently announced National Infrastructure Assessment; and Natural Resources Canada’s Energy and Utilities Sector Network has shown interest in the issue.

QSC Recommendations

- 20. The Government should ramp-up its existing awareness-raising efforts to ensure that all sectors of the economy are aware of the quantum threat and fully understand what needs to be done to prepare for it and respond to it.**
- 21. These efforts should involve not just Canada’s national-security agencies, but also the broad array of other departments responsible for vulnerable sectors – such as Finance, Transport, Natural Resources, Infrastructure, and Innovation, Science and Economic Development – that need to commence, broaden or accelerate their efforts in this area.**

Thoughts on *Developing a National Quantum Strategy:* Focusing on the Quantum Threat to Cybersecurity

Question 8. How can we leverage and mobilize Canada's research and business strengths to connect with international partners? How do we ensure we derive maximum benefit from these collaborations?

- Canada currently holds leadership cards in the quantum-safe arena, and we should consider playing them while they still are leadership cards.
- For example, if Canada had wished to be involved in the new AUKUS security alliance with Australia, the United Kingdom and the United States – which is to involve cybersecurity, quantum technologies and artificial intelligence as well as submarines – we could have brought to the table recognized strengths in all three of those areas.

QSC Recommendations

- 22. Canada should consider forging or joining strategic partnerships on quantum readiness, working with international partners with similar outlooks and interests.**
- 23. Security arrangements aside, Canada should consider negotiating and joining a quantum (including quantum-safe) free-trade arrangement with like countries, in particular other middle powers.**
- 24. The Government should encourage and support strong and meaningful Canadian participation at pertinent international standards tables.**

Thoughts on *Developing a National Quantum Strategy:* Focusing on the Quantum Threat to Cybersecurity

Question 9. How should the National Quantum Strategy address emerging security risks and build on Canada's expertise to create commercialization opportunities?

QSC Recommendations

- 25. The National Quantum Strategy should be seen and employed as a very significant opportunity to increase awareness of the quantum threat.**
- 26. The National Quantum Strategy should include effective measures to build the implementation talent pool that we will need to undertake the cryptographic migration to post-quantum cryptography.**
- 27. The National Quantum Strategy should identify the building blocks and milestones that will need to be in place if Canada is to achieve quantum readiness, and then set them out in the form of an implementation roadmap.**

Thoughts on *Developing a National Quantum Strategy:* Focusing on the Quantum Threat to Cybersecurity

Question 10. What specific gaps, barriers and challenges hinder our efforts to solidify Canada as a global leader in quantum technologies?

- With respect to Canada's leadership in post-quantum cryptography / quantum safety, a significant barrier seems to be a lack of support at the most senior levels of government for actions to address the quantum threat, as identified throughout this document; line departments can do only so much without such support.

QSC Recommendation

- 28. Ministerial Mandate Letters should reflect an awareness that the quantum threat is a serious threat to Canada that must be addressed, and should set out the quantum-safe objectives that specific Ministers are expected to achieve.**

Thoughts on *Developing a National Quantum Strategy:* Focusing on the Quantum Threat to Cybersecurity

Question 11. What best practices have you seen in Canada and/or abroad that we should consider when forming an advisory body?

- Best practices for cryptographic migration, as produced under the aegis of the Canadian Forum for Digital Infrastructure Resilience.
- The global process conducted by the National Institute Science and Technology in the United States to identifying viable quantum-safe algorithms.
- The national quantum advisory bodies already in place in the United Kingdom and the United States.

QSC Recommendations

- 29. The Government should name a high-level Canadian quantum advisory board of experts that represent the broad spectrum of quantum-related interests and expertise, including readiness in the face of the quantum threat to cryptography**
- 30. The quantum advisory board, like the eventual National Quantum Strategy, should be designed to be sufficiently agile to deal effectively with rapid developments in science and technology.**
- 31. The quantum advisory board should include at least one senior representative from Quantum-Safe Canada.**

Thoughts on *Developing a National Quantum Strategy:* Focusing on the Quantum Threat to Cybersecurity

Question 12. Are there any considerations that we have missed, questions we should ask or elements we should explore further?

- One set of considerations that needs to be address is the need for technical and community colleges across Canada to collaborate to develop quantum-safe educational modules and offer quantum-safe programs – likely layered on top of existing cybersecurity programs; these matters are discussed below.

Thoughts on *Developing a National Quantum Strategy: Focusing on the Quantum Threat to Cybersecurity*

Supplemental Questions from the National Quantum Strategy Security Roundtable – July 29, 2021

Security concerns over disruptive quantum technologies

Nations across the globe are racing to research, develop and deploy quantum technologies, which have some enormous disruptive potential for upscaling opportunities, as well as serious security concerns and challenges. For example, stable large-qubit-scale quantum computers are on the horizon that will be capable of breaking conventional cryptography, ultimately translating into diminished trust in the digital economy.

- A key point is that without trust there will rightfully be unmitigated concern for the economy in general and the digital economy in particular; this may well translate into commercialization and adoption challenges – and even a ‘funding winter’ – for the quantum-computing industry.
- If we don’t get ahead of the transition to quantum-safe cryptography, there may well be serious calls to control access to dual-use quantum technologies, especially quantum computing.
- However attractive access controls may appear on the surface, they would be very difficult to implement effectively – meaning that restricted technologies would still leak out to our adversaries, while potential domestic users would face higher prices and lose access to beneficial aspects of quantum technologies.

QSC Recommendation

- 32. The Government should do what it can to ensure that special restrictions quantum cryptography are removed from the Wassenaar Arrangement.**

Thoughts on *Developing a National Quantum Strategy:* Focusing on the Quantum Threat to Cybersecurity

Question 13. With regard to the security aspects and implications of research, development and deployment of products based on quantum technologies (e.g., sensors, computers), what should Canada’s national quantum strategy target in the next three years and beyond?

- As noted above, the greater need is security from quantum computers, as opposed to the security of quantum computers.

QSC Recommendations

- 33. A prime focus of the National Quantum Strategy over the next three years should be considering, encouraging and facilitating the necessary migration of the cryptographic base to quantum-safe cryptography.**
- 34. Beyond that, a focus on “products based on quantum technologies” should include quantum cryptography.**

Thoughts on *Developing a National Quantum Strategy:* Focusing on the Quantum Threat to Cybersecurity

Quantum [and other] supply chains

Question 14. How should Canada ensure, to the greatest extent possible, both research security and reliable and secure supply chains for the Canadian quantum internet and for Canadian quantum applications?

- The larger issue of the security of Canadian society and Canada's economy in the face of quantum computing and the quantum threat should not be overlooked in the National Quantum Strategy.
- Since the major looming threat to critical infrastructure (CI) and CI supply chains is the quantum threat to the cryptography that underpins cybersecurity, this should be a key area of concern for the quantum industry and the National Quantum Strategy.
- For years to come, reliable and secure supply chains for Canada's CI sectors are likely to take precedence over supply chains for the quantum internet and/or quantum applications.
- All sectors of the Canadian economy, especially CI sectors, will need meaningful quantum-readiness strategies and action plans.
- Implementation of these strategies and plans will involve coherent and timely migration from existing quantum-vulnerable cryptography to cryptographic agility and post-quantum cryptography.
- This will necessitate the replacement of classical cryptographic hardware and software with quantum-safe and cryptographically agile hardware and software.
- The massive move to upgrade and replace should be of great benefit to the Canadian and global quantum-computing industry, but only if the sectors and organizations being upgraded 'get there' on time; if they don't, they may not even survive – to the benefit of those who do not wish us well.

QSC Recommendations

- 35. Government should encourage and, where possible, compel all sectors of the Canadian economy to develop meaningful strategies and action plans that will drive coherent and timely migration from existing quantum-vulnerable cryptography to cryptographic agility and post-quantum cryptography.**
- 36. Beyond the Government itself, this work should start with CI sectors where the Government possess significant regulatory powers, for example banking, telecommunications and airlines.**

Thoughts on *Developing a National Quantum Strategy:* Focusing on the Quantum Threat to Cybersecurity

Question 15. Are there specific capabilities that Canada should invest in to reduce national security risks and/or dependence on other countries for Canada's quantum needs? Are there quantum technology applications with special or higher security requirements?

- Cryptographic systems and modules are at the basis of securing digital platforms, and thus it is of the utmost importance for our national security and economic security that quantum-safe cryptography technologies are both available and trustworthy.

QSC Recommendations

- 37. In order to reduce national security risks in the quantum age, the Government must move quickly to raise awareness of the quantum threat and encourage the development and implementation of sectoral quantum-safe strategies and action plans for the necessary migration of the cryptographic base to quantum-safe cryptography – as stressed above in greater detail.**
- 38. If Canada is to 'get its own house in order' regarding quantum readiness, as opposed to waiting in line for foreign experts to come help us after they've taken care of their home countries, then serious and sustained funding will need to be directed to the development of a greatly expanded domestic cadre of risk-assessment, systems-integration and cybersecurity experts with superior quantum-safe skills; if we do this soon enough, it will be other countries who will be relying on our Canadian experts to help them – to the considerable economic benefit of Canada.**

Thoughts on *Developing a National Quantum Strategy: Focusing on the Quantum Threat to Cybersecurity*

Skills and talent

Question 16. How can Canada develop, attract and retain sufficient and diverse talent to ensure informed strategic leadership and sound policy making with respect to quantum technologies?

- Canada must move quickly to assemble the large cadre of risk-assessment, systems-integration and cybersecurity professionals with strong quantum-safe skills that will be needed to implement the action plans.
- As education is a provincial matter in Canada, the role of the federal government may be limited to encouraging provinces and territories – perhaps via the Council of Ministers of Education, Canada – to work together to develop quantum-safe modules and course materials that can be incorporated into college-level cybersecurity programs, and funding efforts to train the trainers.
- The Government could also fund college-level research into matters such as the quantum-safe skills gap and the number and content of courses and programs needed to fill that gap in the hope that this will spur colleges to act on the results of that research.
- Certification processes for quantum-safe programs and graduates will be needed to assure employers (and ultimately the public) that graduates are properly prepared to undertake the work required; ideally these would be national in scope – perhaps building on existing efforts involving CyberSecure Canada and the CIO Strategy Council – but will be tied to provincial and territorial training programs.

QSC Recommendation

39. The Government should identify measures to encourage Canada's provinces and territories to invest in the following:

- **The introduction of quantum-safe programs and modules (including risk assessment / management) in technical colleges across Canada, and possibly private training colleges.**
- **The development of quantum-safe training modules and course materials for those technical colleges, etc., likely as an overlay to existing cybersecurity programs.**
- **The development and introduction of train-the-trainer programs, and certification processes for quantum-safe programs and graduates.**

Thoughts on *Developing a National Quantum Strategy: Focusing on the Quantum Threat to Cybersecurity*

Question 17. How can Canada develop, attract and retain sufficient and diverse cybersecurity talent to ensure continued skilled support in areas that will produce quantum technologies and lead to their adoption?

- This question appears to address the development, attraction and retention to highly skilled research personnel for the quantum sector, as opposed to the implementation skills discussed above, we will follow suit.
- It is critically important that Canada's highly skilled cybersecurity research talent focus not just on supporting the production of quantum technologies but also on developing solutions that protect society from the downside of quantum computing, the quantum threat to cryptography.
- Canada is a world leader in certain areas, though government funding needs to focus more on the practical / adoption side of our researchers' work, and not just the fundamental / theoretical side.
- In general, government should not rely on matching mechanisms in any public strategy when it comes to funding core elements that serve the common good.
- In addition, there should be targeted funding for research that bridges quantum technology and real-world applications in cybersecurity, bringing in real-world networking and cybersecurity experts to work alongside academic quantum researchers who are less attuned to business needs; neither side can do what's needed alone.

QSC Recommendations

- 40. The Government should fund at least five new research chairs in quantum-safe cryptography at Canadian universities.**
- 41. The Government should enhance existing funding programs available to Canadian-based university researchers in quantum cryptography and quantum key distribution, especially those working on practical applications and integration into real-world networks.**
- 42. The Government should encourage and support the expansion of the Quantum School for Young Students (until recently the Quantum Cryptography School for Young Students) at the high-school level.**
- 43. The Government should sponsor the CryptoWorks21 and similar programs outright, rather than via a 'matching formula'; such support could apply to similar programs adapted for the undergraduate level.**